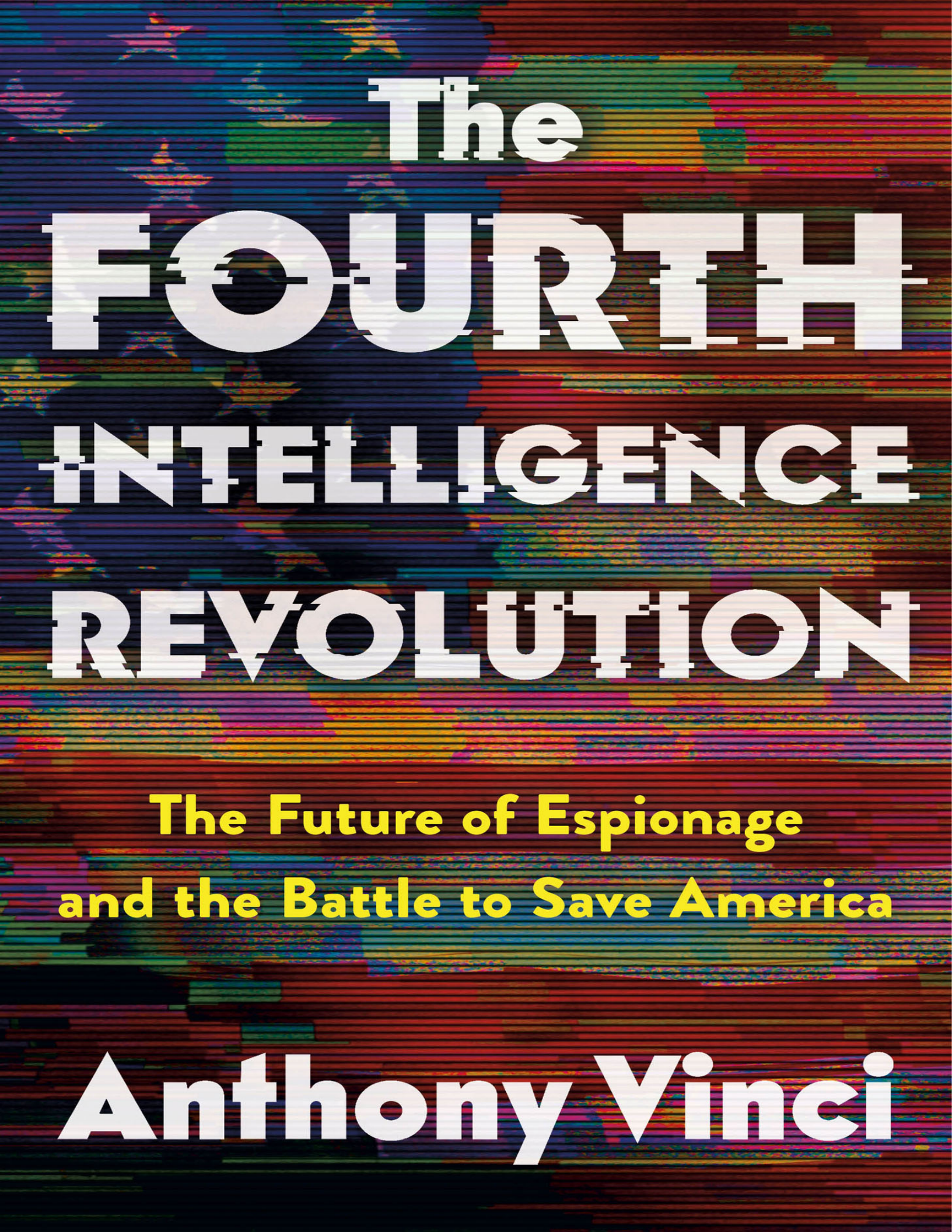
The
FOURTH
INTELLIGENCE
REVOLUTION
The Future of Espionage
and the Battle to Save America
Anthony Vinci

The FOURTH INTELLIGENCE REVOLUTION

The Future of Espionage
and the Battle to Save America

Anthony Vinci

HENRY HOLT AND COMPANY
NEW YORK

OceanofPDF.com

Begin Reading

Table of Contents

About the Author

Copyright Page

Thank you for buying this
Henry Holt and Company ebook.

To receive special offers, bonus content,
and info on new releases and other great reads,
sign up for our newsletters.

Sign Up

Or visit us online at
us.macmillan.com/newslettersignup

For email updates on the author, click here.

OceanofPDF.com

The author and publisher have provided this e-book to you for your personal use only. You may not make this e-book publicly available in any way. **Copyright infringement is against the law. If you believe the copy of this e-book you are reading infringes on the author's copyright, please notify the publisher at: us.macmillanusa.com/piracy.**

OceanofPDF.com

For H and C

And all those who serve in secret

OceanofPDF.com

Prologue

From 350 miles up, a satellite unfolds its origami-like antenna, sending out an electromagnetic wave pulse that cuts through the dark and fog unchallenged. The signal ricochets off a Russian T-80 tank lumbering through the Dnieper River valley in Ukraine and is received back by the antenna, which captures the tank's image and even its speed. The satellite uses synthetic aperture radar, or SAR, a relative of the radar used by the dishes spinning around at airports to track airplanes. With such satellites, the cover of night no longer affords protection from espionage.

In the most paranoid days of the Cold War, the best Soviet and American scientists developed a way to spot each other's nuclear weapons regardless of weather or darkness. A constant eye from the heavens, unburdened by the need for light, satellites ensured continual vigilance and allowed Soviet and American generals to sleep a little easier.

But the commercial SAR satellite now hovering above Ukraine is not the government-operated, multibillion-dollar, bus-size satellite of the past. This smaller sibling, built by twenty-something-year-old aerospace engineers wearing hoodies and jeans in a factory outside Denver, is owned by a tech start-up. Instead of being beamed down into a massive dish hidden in a military base and connected to a highly secure underground bunker, the images go through a private relay ground station on the icy island of Svalbard, not far from the North Pole. From there they travel along the same optical cables that carry our website clicks under oceans to a database hosted in cloud servers somewhere in suburban Virginia. Nestled in the cloud, a machine learning–based artificial intelligence system runs

analytics on the images. Then the information retraces its steps and is beamed back to space. A Starlink low-earth-orbit telecommunications satellite, owned by the private company SpaceX, bounces the data back down to a receiver mounted on top of a rusty, thirty-year-old pickup truck parked next to a muddy trench in Ukraine. The whole process takes mere minutes.

When the imagery comes in, a Ukrainian intelligence officer who is younger than the iPhone quickly extracts coordinates from the file and relays them to her drone operator companion. The drone at hand is not the multimillion-dollar MQ-1 Predator that used to hunt terrorists over the canyons outside Kandahar. Instead, it's a tiny craft bought for a few thousand dollars from a hobbyist company, small enough to be pulled from a backpack, with a mounted camera repurposed from an older-generation cell phone. The drone operator wears cyberpunk goggles that project the drone's view directly into his eyes. He uses a handheld control, not unlike the one used to play Xbox, to send the drone off toward the tank. As the sun rises and the fog burns off, the drone flies over, providing real-time reconnaissance for a High Mobility Artillery Rocket System. The deadly HIMARS can launch half a dozen missiles from its camouflage frame from miles away.

While appearing to fly through clear skies, the drone in fact soars across a chaotic battlefield of electronic warfare. From miles away, a Russian electronic warfare unit employs sophisticated sensors to detect any radio waves and sends back powerful electromagnetic radiation to jam any communications with drones and even to overwhelm GPS signals. The Ukrainians know this and have enabled autonomous technology to let the drone continue to detect its environment and fly while being attacked by such electronic warfare weapons. Many drones crash from these electronic warfare attacks, or, worse, their signals lead back to their operators, who are fired upon. But not today.

The drone, with its four spinning rotors, sails through the barrage and sends back the images, coordinates, and headings of the T-80. The HIMARS crew flies into action, inputting the data into the targeting

computer. The missile is launched. It hits its target. The tank is destroyed in a fireball.

The Ukrainians have already left the scene, fearful of a counterattack, but the drone continues to film. Afterward, the imagery gets uploaded to a social media account. Groups on Reddit and other platforms follow the war, donating money to help buy more drones or simply pushing out the images through channels on social media so others can discover what is happening.

Yet these flickering images on social media are not always what they seem. A covert Russian disinformation cell takes the uploaded imagery, alters it using AI to make it look like a Ukrainian tank was hit, and reposts it widely. The social media back-and-forth then becomes the battlefield as well. As the Russian cell enlists more and more bots to post the falsified image, it overwhelms the more truthful image. Social media viewers are left unsure which is the real image and which is fake. An online group of volunteer investigative journalists reverse-engineer the footage to show that it was doctored and repost the original imagery, revealing a Russian disinformation campaign. Other Russian covert disinformation cells play up this disagreement among those for and against the Ukraine war, who believe or do not believe in the image, to further social division here at home.

Though they are thousands of miles away, the war on the physical battlefield and the war on the information battlefield are inextricably linked. Indeed, you may personally have been on this information battlefield at some point, viewing an image or reading a story and considering whether it was true or false. Whether or not you realize it, your decision to forward this image or not becomes another action in the ongoing virtual and real wars. From our couches and bedrooms, scrolling and sharing images on phones and laptops, we are all part not just of the Ukraine war but of a much wider global intelligence war.

As the science fiction author William Gibson once said, “The future is already here, it’s just not very evenly distributed.” This is what modern warfare and intelligence look like. They are a mixture of the past and present. There are officers in Ukraine who stand guard on a battlefield that would be recognizable to a World War I soldier: trenches dug into frozen

ground, stretching for miles; tank treads in the mud; rifles and grenade launchers leaning against farm fence posts; human runners carrying notes. But overhead, drones now fly without pilots, and soldiers carry phones with more computing power than not that many decades ago the entire world had combined, using them to analyze images from tiny satellites zooming overhead in real time.

Wars offer a glimpse of the future, and in this case, we can see a window into the future of intelligence. What is happening in Ukraine is happening not just there. These tactics, techniques, and procedures now at work in Ukraine—or TTPs, as people in the military and intelligence world call them—are being adopted by many governments around the world. A war in Taiwan will be ten times what we see now, just as World War II was a leap ahead from what was observed in the 1930s with the Spanish Civil War. But also, just as World War II led to widespread use of radios and aerial surveillance and computers in the civilian world, the same is happening now. What's happening in Ukraine with AI and surveillance and disinformation is entering our everyday world. It is a preview of what's to come for all of us.

What is unique about this future is that not only is it here, but it is accessible to anyone. You don't need to own a billion-dollar satellite; you can close this book, open your phone, and go online to see the imagery yourself, quite a bit of it completely for free, just by typing into Google "purchase satellite imagery." Try it. Once, you needed access to a MQ-1 Predator drone flown by pilots at Creech Air Force Base in Nevada to get aerial images of forbidding territory. Today, you can buy a reasonably good drone for a few thousand dollars. Once, you needed a highly trained imagery analyst to understand what you were seeing on a blurry satellite image. Today, you can download a selection of analyst toolkits made by small Silicon Valley companies that will decipher it for you.

This sounds amazing, and it is, but it can also be terrifying, because intelligence cuts both ways. It once took highly trained and very rare technicians to doctor images. Now anyone can do it from their cell phone. Whereas once disinformation was a rarity, it is now commonplace. The ubiquity of sensors—in your phone, your smart home devices, and your car

—means there is no longer a need for wiretaps. Your life can be recorded anywhere at any time and accessed by anyone with the tools or authority to do so. Intelligence is now everywhere in our lives.

This book is a tour of the present and future of espionage. Intelligence is both more technological and more open to the public. It is becoming democratized. It is not only far different from the intelligence we imagine from the golden age of the Cold War, but also far different from the intelligence I was trained to do two decades ago. We are experiencing a revolution in intelligence. It's not the first such revolution, but it may be the most important one. This one affects not just intelligence officers and intelligence agencies, but us all. It is for this reason that I am writing this book.

It feels a bit weird to be speaking publicly about these topics. Our training as intelligence officers comes down to a single lesson: You do not talk about Fight Club. But the only way to make intelligence better, to better protect the nation, is to widen the audience and the debate. A few agency directors and policymakers cannot envision the future in the way that the hive mind of a large swath of people can. Moreover, the democratization of intelligence means we must all be responsible for the system. We can't do that if we don't know what's going on. In the words of intelligence, we all have a "need to know."

This book is written partially for those who have always had a need to know—those professionals who run intelligence operations or whole agencies and the generals, policymakers, and politicians who make decisions about what our agencies should and should not do. I have a point of view that many might find controversial or, perhaps, just plain wrong. But I hope to continue my service to the nation by providing a new perspective on the future of intelligence and what must be done to ensure that intelligence agencies keep pace with that future.

At the same time, this book is also for everyone else, who I believe now should have a need to know. We all should have a view of what intelligence is and can be. There are stark moral choices to be made. What our agencies do reflects our national morals. And ultimately, these agencies

are governed by us as voters and citizens. In that regard, we should all understand intelligence and have a viewpoint.

Understanding intelligence isn't just about knowing what all the agency acronyms stand for or learning about some obscure, action-packed field operation. The first area is for academics and policy wonks; the second is the domain of historians and thriller writers. To me, understanding modern intelligence is about learning how to think like an intelligence officer and viewing the world of intelligence competition through a new lens. And once you've seen it this new way, you can't unsee it. Those news blips about TikTok and Chinese space planes and Russian hackers will connect and coalesce for you, increasing your understanding of what the real threats are, to all of us as individual citizens of a democratic world.

When you begin to think and see like an intelligence officer, you will see the whole world differently. A poorly written but highly opinionated article might be part of an information operation. A company with no known employees or recognizable customers might be a front for economic espionage. A chalk mark on a random brick wall might be the signal for a clandestine meeting. So think of this book as a new lens on the world.

Once you've read this book and seen all the crazy, dangerous things going on, I hope you'll want to do the right thing and play your part. For some, that might mean one day signing up to be an intelligence officer. For others, it might mean considering whether your company's product could be used to do some good for the nation. For many, it means deciding whether to forward that doctored image. For all of us, it means taking part in an educated debate about what our intelligence agencies should and shouldn't do and voting to make that so. Intelligence is often a matter of ethics, and it is not only the ethics of intelligence agency directors in Washington, DC, that counts. The ethics we all have as individuals matters, too. Whatever you decide to do with the information revealed to you here, I hope this book's insights will empower you to see the world for what it is and to do something about it.

OceanofPDF.com

Introduction

Nations abhor secrets like nature abhors a vacuum. Secrets can be so dangerous that nations will do anything to uncover the truth behind them. Pursuing these secrets isn't the domain only of presidents trying to avert nuclear war, but also of you, me, and our families. Adversaries' threats don't just happen in a desert or jungle thousands of miles away; they now happen in our towns, our communities, and even our living rooms. The pursuit of secrets is a public good and is why, generation after generation, people have taken on the mission to reveal the truth. I was one of them.

Despite my training as an intelligence officer, I never expected to carry a gun; that was what soldiers did. But 9/11 changed everything. In 2008, I was serving in Iraq as an operations officer (often called a case officer), charged with finding, assessing, recruiting, and handling intelligence sources. I carried a SIG Sauer 226 sidearm and an HK416 rifle with an Aimpoint site for close-quarter combat. My fellow officers and I rode around in Level 7 up-armored, low-pro vehicles that could take multiple shots from an AK-47 assault rifle while also being indistinguishable from other cars on the road. On the street, I blended in with the local Iraqis by sporting a dark tan, a black-and-white checkered keffiyeh scarf, and a pair of aviator sunglasses. The only real technology I had were my radio and cell phone. In Baghdad, my days consisted of maneuvering around the city, dodging insurgents, meeting sources, debriefing those sources for intelligence, and reporting what I learned back up to the generals in the Green Zone or to politicians in DC.

This was the way we used to do intelligence work.

Fast-forward to 2017. I was back at work in the Intelligence Community—the IC, as it has become called by most intelligence officers—but this time, behind a sizeable desk as the first chief technology officer and associate director of capabilities of the National Geospatial-Intelligence Agency (NGA). Instead of running operations on the street, I was now in charge of all the agency's technology, R&D, contracting, budget, and strategy. Awestruck and overwhelmed, I knew that with the keys to the kingdom came great responsibility. On my first week in the role, my boss, Director Robert Cardillo, gave me one mission: modernize us before it's too late.

The NGA and its precursor agencies were devised to provide critical aerial and satellite imagery analysis and maps to presidents and generals, soldiers and civilians. The NGA's job was to see what was happening behind enemy lines and to head off threats—essentially, to ensure that the United States was not surprised. The NGA was once the cutting-edge master of its domain. Think analysts in rolled-up shirtsleeves and skinny ties smoking unfiltered cigarettes while poring over U-2 photos of Soviet missiles during the Cold War. When I say the NGA *was* the master of its domain, the past tense is intentional. When I started, there was no more tobacco, most people wore J.Crew business casual, and analysts tediously zoomed in on computer monitors. Like many people raised on 007 and *Mission Impossible*, I once assumed the CIA and other intelligence agencies were the possessors of the very best technology. I've now learned better. Today, the private sector, especially Silicon Valley, is responsible for many of the most important innovations in intelligence.

From my earliest days at the NGA, I saw that no matter how many analysts we packed into the giant headquarters tucked away on a nondescript military base, there was no way we could possibly analyze the overwhelming number of images coming in every day from government satellites. And that says nothing of all the imagery arriving from an exponentially growing number of commercial satellites, plus all the drones buzzing around the world. As Cardillo put it in 2017, "If we were to attempt to manually exploit the commercial satellite imagery we expect to have over the next 20 years, we would need eight million imagery analysts." In a

world of ever-present potential terrorist attacks, Chinese hypersonic nuclear-tipped missiles, and other existential threats, this was a major problem.

I'd previously run clandestine missions riding shotgun in armored vehicles in Iraq, walking dusty alleyways in African countries, and looking out from gleaming sky-rises in Asia. But I'd never encountered anything like this. Actually, when it came to tackling this mission at the NGA, my more relevant experience came not from the field, but from a trendy loft in Lower Manhattan. Not long after returning from Iraq, I'd left the world of intelligence, recruited a team of superstar programmers, raised some venture capital, and had some success founding and running tech start-ups. Now back inside the IC, at this lumbering behemoth of an agency, I knew I'd need to do something similar: recruit the best minds already working on the cutting edge and send them on a mission much harder than making a cool app.

In the fall of 2017, at a dinner at a hip San Francisco restaurant hosted by a close friend who was both a venture capital investor and a former Army officer. I sat down with several very smart, very ambitious, and very young leaders of companies that were pushing the envelope. One was designing radars to track space junk before it hit a satellite or an astronaut in the International Space Station. Another was applying AI to the analysis of vast quantities of global satellite imagery in a fraction of the time it had taken previously. A third was building ridiculously small and inexpensive satellites that could collect SAR images. All these were once thought to be impossible feats.

These were the right people to help me fix the agency's technology problem. But their companies were at nowhere near the scale necessary to make change happen inside a multibillion-dollar agency working in two war zones with officers across the world. Their collective budgets at that time were tiny, equivalent to a fraction of the cost of a single F-22 Raptor fighter jet. When we met, these firms were still such outsiders that they had no chance of landing U.S. government contracts. Getting them into the agency meant helping them scale using esoteric government acquisition and partnership vehicles like Other Transaction Authorities, or OTAs, and

Cooperative Research and Development Agreements. Although imperfect, it was the best path we had, and we made use of it. Fast-forward five years, and all these companies have raised hundreds of millions of dollars, are selling their technology to the U.S. government, and are having a major impact on the Intelligence Community.

One of the companies I ran across at the dinner that evening, Capella Space, manufactured and operated SAR satellites for commercial purposes. The company's arcane knowledge behind the intricate folding motions of expandable space antennas, combined with the efficiencies and innovations of the tech start-up mind-set, led to breakthroughs. SAR satellites used to cost billions of dollars and were operated secretly by the United States and the Soviet Union, while these satellites cost about the same as a one-bedroom apartment in San Francisco, and today, almost any company in the world can buy their images. Capella and other commercial satellite companies like it are transforming intelligence by adding new innovations, bringing down the cost of intelligence collection, and increasing the number of sensors available, not just in the United States but also in Ukraine, Japan, and elsewhere.

It's not just commercial satellites that are transforming espionage. Artificial intelligence—technology owned almost exclusively by private tech companies, not government agencies—is used regularly to analyze the tsunami of data coming out of those satellites and the countless other sensors. Autonomous drones are already here and revolutionizing war and intelligence. And a whole new generation of cyberattacks and disinformation built upon AI threatens the United States and requires new technology approaches to defend against it.

When I rejoined the Intelligence Community, little did I realize that I was at ground zero of a revolution in intelligence, nor that I would become one of its biggest agitators. This latest transformation in how we gather and analyze intelligence had already started before I joined as CTO of the NGA. It's now clear that the changes I pushed for at the agency were ultimately part of something much larger. The commercial satellite imagery and the other technologies I first witnessed in Silicon Valley were just the tip of the

spear in the coming intelligence revolution, a revolution that would soon expand and accelerate.

But what I have since come to realize is that this intelligence revolution is about much more than just technology. Global intelligence competition has created a paradigm shift in intelligence that expands espionage to include everything from economics to human rights abuses to biotechnology to the far side of the Moon. This competition is driven by the authoritarian adversaries, especially China, who have turned toward asymmetric means to threaten the United States and the West. Most pressing, this new competition is targeted at all of us. Authoritarians have come to realize that democracies are ruled by the people. Intelligence targets rulers. Therefore, everyday people in the United States and, now, most of the world are the target.

The intelligence revolution is about a shift to a world in which all of us —not just those who work in the IC—must become like intelligence officers. Social media and the powerful sensor packages represented by our smartphones make all of us potential targets of espionage. But more than that, we are all also increasingly doing at least some of the work of intelligence officers in that we are responsible for protecting ourselves, our families, our neighbors, and our nation from adversaries who would try to steal our most intimate personal information, wreck our democratic processes, and degrade our most basic human rights. What is hopeful about this alarming turn of events is that we now have most of the tools we need to protect ourselves and a voice in the conversation about what the United States needs to do to make itself more secure. This is a view of intelligence that is unrecognizable even to those at the top of our intelligence agencies.

★ ★ ★

To understand today’s intelligence revolution requires a look back at how we got here. Everyone keeps secrets. Countries are no different. And though some country secrets are innocuous, others could ignite global conflict. Other countries want our secrets, and they try to steal them. We try to protect our secrets and then try to steal theirs. This is the basis of intelligence—a constant competition for secrets. We try to obtain the secrets

of others, they protect them, and we figure out a new way to obtain them that is not protected. They do the same to us, and it's spy versus spy, ad infinitum. But the means of spying constantly evolve, based on new defenses, new threats, new technology, and new social changes.

This competition over intelligence is as old as time. We have always needed to know about our enemies, their movements, their numbers, and their assets. As Phoenician or Renaissance-era explorers crossed vast tracts of forbidding land or set sail on epic voyages, they made intricate maps of landforms and previously unknown settlements, taking note of who lived there and what their politics were. Capturing this information was essential for planning military conquests and trade routes. Explorers and their governments also kept watch for competing nations' similar explorations and reconnaissance. Court intrigue, whether in Ancient Rome or Habsburg-era Vienna, has always been of interest, and spies were always sent to see what was going on.

This nature of intelligence remains the same. Intelligence concerns information about real or potential threats that can help us make better decisions. But, really, when you get right down to it, intelligence is about secrets. Intelligence officers specialize in finding out what is not known and what is protected from being known. Secrets go both ways, and intelligence agencies also deal with protecting secrets—meaning there is intelligence and counterintelligence. Finally, intelligence also concerns the use of covert actions to secretly alter information or events. Though the core mission may remain the same, the character of intelligence changes over time, leading to new intelligence revolutions. For the United States, though our intelligence journey goes back to the birth of the nation, it's World War II where our modern conception of intelligence was born.

There have been three distinct eras of intelligence since World War II. After the heroic era of our battles in Europe and the Pacific came the golden age of intelligence in the Cold War and, most recently, the chaotic era that arose from the attacks of 9/11 and the wars in Iraq and Afghanistan. We are now living through the fourth and most consequential and rapid era of change. While each of these periods has been marked by its own events and

technological developments, there are common trends that connect them in a continuum.

From the Axis powers in World War II, to the USSR in the Cold War, to Al-Qaeda in the war on terror, to our current tensions with China, the United States has always faced an *autocratic adversary*. These adversaries have represented a challenge to freedom and democracy and created an urgent need for transformation. Threats from autocratic adversaries caused the creation of the first U.S. intelligence agency, the Office of Strategic Services, or OSS, and the professionalization, scaling, and multiplication of that agency into the Central Intelligence Agency, the National Security Agency, the National Reconnaissance Office, the Defense Intelligence Agency, and other agencies during the Cold War and, after 9/11, the creation of an entire Intelligence Community of agencies.

There has also, over the course of the last century, been a series of trends in intelligence.

There has been an expansion of intelligence targets. Intelligence was military-focused during World War II and became militarily and politically focused during the Cold War, with spies operating out of embassies worldwide. Post 9/11, intelligence went beyond nation-states to include non-state terrorists and beyond government targets to include things like infrastructure and transportation.

Intelligence has become less secret over time. During the Cold War, intelligence was ultra-secret. (The NSA's nickname was "No Such Agency.") This secrecy waned post 9/11 as the U.S. government needed to bring in commercial companies to do more of the technological heavy lifting.

We have become, since World War II, far more technology-reliant. During the war, intelligence was still largely a human endeavor, with some occasional technology, like the use of suitcase radios and aerial reconnaissance, mixed in. During the Cold War, technologies for intelligence collection proliferated dramatically, including the use of satellites, submarines, and ELINT (electronic intelligence) sensors. In the post-9/11 era, U.S. agencies, faced with analyzing vast oceans of data, became profoundly dependent on computers.

The definition of who does intelligence has expanded. This started with the formation of a centralizing agency in the form of the OSS, led to massive growth into multiple professional agencies during the Cold War, and then to a whole-of-government intelligence approach in the 9/11 era.

We're now living in the age of disruption, which is transforming the U.S. Intelligence Community for the fourth time in less than a century and pushing each of these trends to its extreme limits. China and, to a lesser extent, Russia, Iran, and North Korea—all autocratic governments determined to harm U.S. interests—are driving this revolution. These adversaries cannot compete with the United States economically, militarily, or diplomatically, our traditional areas of strength. Consequently, they compete with us asymmetrically and expand their subversive operations into areas like economics and finance, science and technology, and information and ideology. Whereas the Soviets once put the United States at risk over an invasion of Western Europe through the strategically important lowlands of central Europe known as the Fulda Gap, now China puts the United States at risk by controlling 5G networks. Meanwhile, Russia uses an avalanche of disinformation to affect the outcome of our elections, turning citizens against citizens. The Fulda Gap is now in your pocket, in the form of a smartphone.

The pressures from these adversaries and a series of new technologies, especially AI and networks, are giving rise to the fourth intelligence revolution. This revolution will be marked by several facets. Intelligence will expand even further, into wider and wider parts of society. Technology will play an even bigger role, especially AI, which will automate more and more of intelligence until we reach a point where machines spy on machines. Networking and sensor technologies will proliferate to a point where the whole world may be monitored and we will all become targets of intelligence but also be able to use that same technology to execute intelligence ourselves. This revolution will expand so far that it will be marked by the democratization of intelligence and its incorporation into our personal lives to a point where we will all effectively become citizen spies.

Intelligence is expanding into nearly every aspect of social, political, and economic life. It touches on everything from economic warfare and

science and technology competition, to our most intimate private information about our health and genetics, to things like climate change and pandemics. In today's world, the lithographic method that makes a two-nanometer semiconductor may be more important than the classified range of the newest MiG fighter jet.

The most fundamental of all new technologies, artificial intelligence, is driving this revolution in an altogether new way. AI changes the nature of intelligence at a fundamental level, scaling collections to millions of devices through ubiquitous sensors, leading machine analysis to become more human-like every day and pointing the way to a world in which machines spy on other machines. New technology and, in particular, the commercialization of this technology has also meant that intelligence is increasingly open source, collected and analyzed by private companies, start-ups, scientists, and nonprofits. It is accessible to anyone (and anything) with an internet connection, from bored adolescents tracking the flight patterns of billionaires' private jets to autonomous drones searching for military (or civilian) targets.

The democratization of intelligence means that espionage is spreading into our workplaces and living rooms. Our adversaries have made everyday people their targets because we work at companies that supply our industrial base or vote for leaders who make national security policy. So they target all of us. Today, we all carry around smartphones, little black boxes loaded with sensors and trackers that monitor and share our whereabouts, our habits, and our dirty pics with anyone able to unlock them. These include nefarious actors half a world away, who seek to control, manipulate, extort, and distort the rule of law. That social media post you write or even just "like" is fodder for a foreign power's disinformation campaign. The company you work for could be making technology that is used by intelligence agencies; or the person sitting next to you might be selling your company's secrets to foreign spies. There's a good chance the computer you use every day to stream movies or shop online has Chinese or Russian spyware on it. If you imagined a spy from a hostile country sitting next to you on the couch while you mindlessly scrolled through Facebook or TikTok or LinkedIn, you wouldn't be far off.

Alarmingly, AI and network technologies will be used to fight "cognitive warfare" against you and me, where adversaries will try to change our minds and intentions to their benefit without us knowing. Eventually, this will be accomplished by AI systems that will in effect hack our minds in the pursuit of our adversaries' geopolitical goals. In the end, disinformation will become so ingrained in our world that we will experience a state in which we can no longer tell what is true from false.

But we are not helpless. Awareness about the intelligence targeted at us and the era in which we live is the first step toward taking action to protect ourselves, our families, our communities, and our country. This awareness will help us to see intelligence operations and information attacks for what they are. We can then defend ourselves by using some of the same techniques as intelligence officers and ultimately become citizen intelligence officers. Doing so will not only help us as individuals or communities but the nation as a whole, by making our total national security more resilient.

The stakes are high. The threat of war is real. Conflict could erupt over Taiwan in the not-too-distant future. Already, a major land war is under way in Europe, something we have not seen in decades. The war between Israel and Hamas has led to further destabilization of an already unstable region. What's more, China, Russia, Iran, and North Korea are increasingly joining forces. These de facto alliances could form the basis for World War III. We must remember that intelligence doesn't just help win wars; it is meant to help ensure that wars don't start in the first place.

Another equally terrifying, if more abstract, threat is in the ether. What if the aforementioned autocratic nations ate away at our social, political, and ethical foundations and irreparably undermined and transformed liberal democratic society? By redefining human rights and participating in atrocities that we thought we'd seen the end of, like concentration camps and genocide, China is trying not only to control its own citizens, but also to change international norms in its favor. To fan the fires of social unrest, Russia is actively undermining the democratic process in the United States and beyond. And both countries, and their allies Iran and North Korea, would love nothing more than to cause the long-term weakening, if not

outright dissolution, of the United States and the West. For these autocratic nations, intelligence is not a tool to prevent wars; it is an asymmetric means of attack that can be used on all of us.

Combating these ever-evolving and ever-expanding threats demands two things: we must embrace the democratization of intelligence and rapidly learn to apply new technologies in responsible ways. Adapting to this new world will not be easy. My experience of trying to push the National Geospatial-Intelligence Agency forward to embrace AI and commercial technology was fraught with bitter strife. At times, I was literally yelled at by those who sought to protect their budgets and traditional ways of doing things. The NGA is not alone in this: every agency has similar antibodies (as they are called in Washington) that fight change. They do this not because they don't want to protect Americans and U.S. interests; they have devoted their lives to doing exactly that. The resistance to change comes because the level of change required upends everything they were taught about the systems and processes that once helped achieve that objective of keeping us safe. This lag between the belief that the old system keeps us safe and the reality that it does not is what holds us back.

Our empowerment is the most important part of this intelligence revolution because we all also have a duty to ensure that it occurs in an ethical manner. The philosopher Friedrich Nietzsche once mused that "whoever fights monsters should see to it that in the process he does not become a monster." Today, the United States is fighting monsters, and the only way to ensure that it does not also, in the process, become monstrous itself is for the majority of its citizens to be engaged. We must acknowledge what is happening, pay attention, and actively question ends and means. Most of us want our government to stay out of our personal lives. And most intelligence officers I know—me included—definitely do not want to spy on every U.S. citizen. Every American must work to ensure that this doesn't happen by actively understanding and participating in what is going on and taking part in the conversation, so that the U.S. agencies behave in ways that best defend the United States and protect its ideals. In the end, this book will show that as citizens and voters, employees and taxpayers, we *all*

have a role to play in our national security and are ultimately responsible for the ethics of what our intelligence agencies do.

A world in which AI spies on AI feels like a dystopian science fiction movie. The fact that every facet of our society, from our economy to our scientists to our education systems, is now part of the Great Game of espionage can feel daunting. The idea that intelligence involves all of us, that we are being spied on in our living rooms, that we may all become intelligence officers, may and should make you deeply uncomfortable. But it is an unfortunate reality of where the world is going.

Nonetheless, as scary as the rise of AI and the democratizing of intelligence may seem, you should also feel empowered by it. The United States remains the most powerful nation in the world, and we can defend ourselves from all threats foreign and domestic. Democratizing intelligence also means you have a seat at the table instead of being the passive bystander of years past. You have something to say about how intelligence is done, what technologies can and should be used, and what legal and ethical limits should be maintained. You can also learn to protect yourself from these threats. And this is fundamentally the most important part of this revolution—the fact that we are all in it together. Intelligence is expanding from our whole government to our whole nation to all of us.

This is a story about a revolution in which *we are all the revolutionaries*. In the ways we share and spread information online, in the ways we participate in being surveilled and monitored consciously and inadvertently, in the ways we participate in a globalized economy—we are all involved, whether we like it or not. But by being part of the system, we also get to be part of the solution. We get to have a say in making sure that intelligence is done in a manner that makes us feel secure physically but also morally. Today’s intelligence revolution is just the latest chapter in an eternal competition of which we all have always been a part, but this time, we can be the actors, not just the audience.

OceanofPDF.com

1

The Heroic Age

In July 1777, with the Revolutionary War raging, General George Washington drafted a letter to one of his military leaders, New Jersey merchant turned Continental Army officer Colonel Elias Dayton. He wrote, “The necessity of procuring good intelligence is apparent and need not be further urged—All that remains for me to add is, that you keep the whole matter as secret as possible. For upon Secrecy, success depends in most Enterprises of the kind, & for want of it, they are generally defeated, however, well planned.”

Washington knew the value of intelligence. As early as 1775, he had paid a spy to live undercover in Boston and report on British movements using “secret correspondence.” The great general and his Continental Army went on to create spy rings, analyze intelligence gathered on the British, and use that intelligence to evade and attack the Redcoats. Nor did Washington’s appreciation for the value of intelligence end with the war. One of the first requests he made to Congress as president was the establishment of intelligence funding. Congress agreed, setting up the Contingency Fund for Foreign Intercourse in 1790, the United States’ first black budget to be used by presidents for intelligence operations.

But while the United States knew the power of intelligence in war, peace was another matter entirely. The government and most American people maintained a distrust of intelligence in peacetime for decades. It’s a distrust that endures today. Indeed, if you are reading this book and feel a deep skepticism of the CIA, NSA, or other U.S. intelligence activities, you

are not alone. You share a sentiment that has been around since the beginning of the nation.

Intelligence and democracy are often at odds. It's easy to see how intelligence officers might become secret police, and that is something that goes against our fundamental values. Before World War II, spying was considered dirty, even criminal work that was beneath the upper class. Henry L. Stimson, who served as secretary of war under three presidents and secretary of state under a fourth, once famously noted, "Gentlemen do not read each other's mail."

While Stimson's quote has been taken out of context here—he was talking about spying on allies, not adversaries—this patrician sentiment regarding intelligence was widely shared and left a long legacy. Throughout the eighteenth, nineteenth, and early twentieth centuries, U.S. intelligence was almost solely a military affair, one whose purpose was to find and locate the enemy on the battlefield. In fact, there was no permanent intelligence office until 1882, when the Office of Naval Intelligence was created to collect intelligence on foreign navies, with the Army setting up its own Military Intelligence Division shortly thereafter. The Black Chamber, established after World War I as the first peacetime intelligence operation for cryptology, didn't last long: Stimson shut it down in 1929. But despite his lack of appetite for peacetime intelligence, even Stimson accepted that dirty tricks and spies were a necessary evil of war. When FDR asked him to be secretary of war for a second time, in 1940, Stimson was all in on intelligence.

With a second great war being waged on fronts in Europe and Asia, President Roosevelt realized that the United States needed a modern intelligence agency, a central provider of intelligence for the Office of the President. On July 11, 1941, encouraged by British prime minister Winston Churchill, who became a true believer in intelligence after World War I, Roosevelt ordered the establishment of the Office of the Coordinator of Information (COI). Luckily, the man he appointed to run it had already been effectively running his own personal intelligence agency for years.

When you enter the CIA's Original Headquarters Building in Langley, Virginia, a life-size statue of this man, William "Wild Bill" Donovan, is

standing there to greet you. It's unsurprising, really, given that Donovan managed to get himself anywhere that mattered—to the jungles of Burma and to the beaches in Normandy on D-Day—despite the protestations of the president, the secretary of the navy, the local OSS bureau chief, and everyone in between. Years later, he traveled through Thailand and Vietnam, concerned the latter might fall to the communists. He wanted to see firsthand how he could prevent this eventuality. The man had a knack for not just witnessing history, but also helping to make it.

Donovan's national security career began in 1918 with him leading the famous Sixty-ninth New York Infantry Regiment in the Battle of Landres-et-Saint Georges, for which he later won a Medal of Honor. After the First World War, he returned to New York, opened his own law firm, and ultimately became the U.S. attorney for the Western District of New York. But Donovan wasn't much of a desk guy. Between the world wars, he traveled throughout Europe, maintaining a network of clients, including British bankers and politicians, and providing the intelligence he gathered on developments in Nazi Germany and Fascist Italy to the United States. On one such mission, he met with the Italian Fascist leader Benito Mussolini, learned about Italy's desire to expand its territory, and was granted permission to visit the front in Italy's war in Ethiopia. Even as Donovan, a lifelong Republican, publicly criticized the Democrat Roosevelt's tenure as governor of New York, the two maintained correspondence on developments in Europe. Roosevelt realized that Donovan's deep knowledge of international affairs and overseas contacts made him the obvious choice to run the nascent COI.

The COI, however, was never a true intelligence agency. Politics still limited how far Roosevelt could go with intelligence, stuck as it was between the paranoia around peacetime intelligence and the jealousy of its mission by the military and the Federal Bureau of Investigation. Rather than gathering intelligence, the COI had as its main functions the coordination of intelligence coming in from the Army, Navy, State Department, and other government sources and the briefing of the president. It wasn't long before the limitations of this approach were made tragically clear.

Pearl Harbor was one of the great intelligence failures in U.S. history. The United States had some warnings of a possible attack, but the information did not make it to Pearl Harbor in time. A fleet of Japanese ships got all the way to Hawaii without anyone noticing. More than two thousand men were killed and nineteen U.S. ships sunk.

On June 13, 1942, with Pearl Harbor fresh in the minds of all Americans, President Roosevelt established the Office of Strategic Services (OSS) through an executive order. He put Donovan in charge. The OSS's formation was a politically complex balancing act. While it notionally reported to the Joint Chiefs of Staff, Donovan's true boss was President Roosevelt. The OSS immediately ran into operational challenges. General Douglas MacArthur, the Pacific commander, did not allow the OSS to operate in the Pacific Theater, and J. Edgar Hoover, the director of the FBI, prevented the OSS from operating in North or South America without his permission or oversight. Nonetheless, the OSS quickly carved out a significant role in intelligence.

The OSS represents the Big Bang of U.S. intelligence. Most of our modern-day intelligence traces its origins, culture, processes, and people to that organization. This was in no small part due to Donovan himself, who proved to be a preternaturally talented leader of spies. He had a knack for recruiting not just the best and brightest, but also the most interesting and qualified. The demographics of the group and their expertise varied widely —from convicted burglars, who could teach safecracking; to stage magicians, who could teach sleight of hand; to the sons and daughters of families included in the Social Register. Observers nicknamed the organization "Oh So Social." Donovan had a different name for its members, "the glorious amateurs." He led these men and women—the OSS included four thousand women, including celebrity chef Julia Child—from the front personally, instilling in them a culture of creativity and a risk-taking approach that led to both costly blunders and surprising successes. And perhaps most important, the OSS established the basic structure for all future U.S. intelligence agencies and codified the intelligence cycle that is still with us today.

The OSS was organized around the basic functions of the modern Intelligence Community: operations, analysis, support, communications, research and development, and counterintelligence. To this day, the CIA is organized into similar directorates; so is the Defense Intelligence Agency and, to one extent or another, most other agencies.

Analysis and operations formed the core of the OSS. On the operational side, the OSS was split between Secret Intelligence (SI), responsible for intelligence collection, and Special Operations (SO), which specialized in covert action and guerrilla operations. This model followed the British example of a secret intelligence function: the Secret Intelligence Service (SIS), also known as MI6, and the Special Operations Executive (SOE). In an unprecedented move, Churchill had the British intelligence service make itself entirely available to Donovan and the OSS to better prepare the Americans. This included sharing the holiest of holies—how to recruit and train operatives and perform covert operations and sabotage.

No one perhaps personified the SI officer quite like the future Director of the CIA Allen Dulles. As a young man, Dulles had been a human intelligence officer during World War I, and when World War II began he welcomed the opportunity to quit his successful legal career and return to the job he loved, the one that would go on to define his life. Dulles was eventually put in charge of OSS's Switzerland office. From this politically neutral perch in the middle of war-torn Europe, he could recruit German officers who likely might be trying to do the same to him. In his biggest success of the war, and perhaps the single biggest OSS success, he negotiated the surrender of around a million German soldiers with Waffen SS Obergruppenführer Karl Wolff.

The SO division was made up of what today we'd call special operations forces. One such unit, the Jedburghs, had three-man teams that included an OSS officer, a radio operator, and someone from the area they were going to. These groups parachuted behind enemy lines in France and surrounding countries, connected with local resistance, radioed information back to invading Allied forces, and sabotaged the enemy. Aaron Bank was one such Jedburgh operator and would go on to help found the U.S. Army Special Forces, also known as the Green Berets.

Once these specialists gathered and relayed intelligence, it was then catalogued and analyzed by the Research and Analysis (R&A) division, led by Harvard historian William Langer. Unlike previous military intelligence analysis offices, the R&A office was meant to focus on all-source analysis, which, as the name implies, included fusing intelligence from a variety of sources, regardless of which agency had collected it. This would become the core approach to analysis in the future and would influence many academic areas, as so many leading professors served in R&A. In fact, the creation of "area studies" as an academic discipline goes back to the organizational structure within the OSS. After the war, many OSS analysts went on to seed academic departments at universities including Harvard and Columbia, and these departments became feeders for the CIA.

The R&D branch of the OSS was tasked with developing technologies for use in operations—think Q from James Bond—ranging from powdered explosives to silencers to wiretaps and suitcase-portable radios. The OSS established the quintessential American approach of leveraging technology for intelligence. When twenty-five-year-old Christian Lambertsen developed and demonstrated an early underwater breathing device, which he called the Lambertsen Amphibious Respiratory Unit (LARU), by swimming around underwater for an hour in the Shoreham Hotel pool in Washington, DC, Donovan immediately saw the value and established the Maritime Unit. Soon, former surfers from the beaches of Los Angeles and Santa Monica were using the devices to infiltrate Japanese-controlled territory to spy and sabotage. These Maritime Unit swimmers would come to be seen as the progenitors of today's Navy SEALs.

As its name implies, the Communications Division focused on communicating with agents in the field. These agents were the first to use so-called suitcase radios, which could be carried by a single soldier and set up behind enemy lines to communicate back to allies—a game changer for intelligence in wartime, which had formally required physically bringing information back to Allied lines. Additionally, as with other intelligence agencies, there was a significant support function designed to recruit and train OSS officers, provide logistics and help to those in the field, and otherwise operate a 13,000-person organization.

Finally, the highly secretive X-2 office was responsible for counterintelligence (CI), operational security, and the subversion of enemy activities. Arguably, the X-2's most important mission was to coordinate with the British ULTRA program, which had decrypted the Nazi Enigma system and was one of the most important sources of intelligence for the Allies. One X-2 officer, James Jesus Angleton, would go on to lead counterintelligence in the CIA and come to define the paranoid counter-communist approach that relentlessly hunted for moles, both real and imagined.

In sum, this is the organization that determined how to securely collect raw information and transform it into actionable intelligence through the intelligence cycle. Today, the intelligence cycle looks similar. It's a continuous loop, one that begins with planning, where decision makers and analysts identify intelligence needs. Collection managers and operational planners determine how best to collect the raw information. Collection might come from open sources, such as news reports, social media, and public documents; or it might happen clandestinely, through human intelligence or satellite or other sensors. Eventually, all that raw data has to be organized and analyzed. For the analysts, it's like a box of scattered puzzle pieces, only there is no picture to tell you how the whole thing is supposed to look in the end. Eventually, their analysis is then collated into reports and briefings. These findings are disseminated to policymakers, military leaders, or law enforcement officials, who then use them to make informed decisions, take action, or develop strategies. These decision makers may also have feedback or suggest new intelligence requirements. As the decision is carried out, the adversary reacts or the dynamics shift, leading to a whole new set of requirements and restarting the cycle.

The OSS's genetic material still exists in the DNA of the CIA and other agencies today. Operations officers at the CIA and elsewhere continue a culture of risk-taking and creativity. From the NSA to the NGA, technology is still fundamental to the way Americans gather intelligence. Today's intelligence agencies are still organized into directorates that resemble those of the OSS. Even the leaders of our intelligence apparatus are legacies of the OSS. No fewer than four future CIA directors and countless intelligence

officers in every agency served in the OSS. Indeed, even by the time I was serving in intelligence, decades after the war, there was still at least one OSS officer in the ranks whom I personally met.

But the end of World War II raised questions about the role of intelligence in a postwar world. Newly inaugurated president Harry Truman recognized the need for organized and centralized intelligence, lamenting that he had no means to coordinate intelligence from around the world or from U.S. territories. However, Donovan's plan for an organization based on covert action and answerable only to the president was too radical for Truman, who was averse to anything that resembled a "Gestapo."

On September 20, 1945, Truman disbanded the OSS. The Research and Analysis branch was absorbed into the Department of State, where it exists today as the Bureau of Intelligence and Research (INR); while the SI and X-2 were moved into the short-lived Strategic Services Unit (SSU) under the Department of War. Most OSS officers were sent back to the military or returned to civilian life.

The OSS might have been replaced, but it is now legend in the world of intelligence. The derring-do and exploits of OSS Special Intelligence and Special Operations officers still hold sway over many of us who later signed up for intelligence service. Their time was truly the heroic age of intelligence. Even by the time I went to "the Farm" (the nickname for the CIA's field craft training facility), decades after the war, OSS officers would come visit and tell us stories. I remember sitting with one at the SRB, the bar at the Farm, and joining the former SO officer in a toast to the fallen over a glass of scotch. As an intelligence officer, I looked up to those in the OSS as the ultimate heroes of the intelligence world. These were the people who risked their lives to win an existential war. Their leaders didn't hide behind bureaucracy, but instead commanded their troops out in the field, showing up in far-flung, dangerous places. They were not afraid of emerging technology—they used their ingenuity to their advantage.

But ultimately, the OSS was short-lived. Like Peter Pan, it never had to grow up and face the realities of an adult intelligence competition. The Cold War would require that U.S. intelligence mature and professionalize, in

order to do battle with the most ruthless intelligence agency the world has ever seen.

OceanofPDF.com

2

The Golden Age

In 1958, the Cold War was heating up. The Soviet Union demanded Allied withdrawal from West Berlin. Sputnik 1, launched at the end of 1957, ushered in the Space Age as the United States raced to catch up. The fear of nuclear war was a constant shadow, with both world powers testing nuclear weapons and developing increasingly sophisticated intercontinental ballistic missiles, or ICBMs, at a breakneck pace.

Amid this crisis, CIA officer Richard Bissell Jr., a key architect of the post–World War II Marshall Plan, was tasked with developing a new reconnaissance aircraft that was sophisticated enough to evade the rapidly improving radar and anti-aircraft technology of the USSR. Working around the clock with the legendary aeronautical engineer Clarence "Kelly" Johnson, who led Lockheed Martin's Skunk Works group, Bissell and his team pushed the new single-jet U-2 from design to flight-ready in an unimaginable eight months. To put that into perspective, the development of the F-35 Lightning fighter took around a decade from concept to flight.

The Lockheed U-2 (nicknamed "the Dragon Lady," after a comic strip character) took its first test flight in 1955 and proved itself a stunningly successful means to collect intelligence. Astonishingly, the U-2 is still in operational use today, although scheduled to be mothballed, flying reconnaissance around the world's hot spots. The U-2 had a simple survival strategy: it soared at over 65,000 feet, higher than any of the Soviet missile systems could shoot. But by the late 1950s, Soviet missile technology had advanced to the point where Soviet anti-aircraft missiles could now reach those altitudes, signaling that the U-2's unchallenged reign was coming to

an end. (In May 1960, pilot Francis Gary Powers would be shot down in a U-2 over the Soviet Union.)

And so, on April 21, 1958, President Dwight D. Eisenhower signed a secret executive order to build the first spy satellites, and in doing so, he changed the course of intelligence forever. The CORONA (originally Discoverer) program was a series of U.S. strategic reconnaissance satellites launched by the CIA between 1959 and 1972 to take secret photos of the Soviet Union and other Cold War hot spots. The CORONA program would become one of the most complex and difficult endeavors ever for intelligence.

After thirteen consecutive failed attempts, Discoverer 14 was launched into a polar orbit from Vandenberg Air Force Base on August 18, 1960, heralding the age of spy satellites. There was no way to digitally transmit the images at the time, so the film was ejected in a satellite return vehicle. Insanely, this vehicle was retrieved by a C-119J Flying Boxcar, which snatched the descending nose cone and its parachute in midair with a fork sprouting from the nose of the plane. Divers waited at the ready, in case the fork missed. The film was developed in secret at Eastman Kodak's Rochester, New York, Hawkeye Plant. It was then analyzed by legendary imagery analyst Arthur Lundhal and his National Photographic Interpretation Center team before finally being presented in person to President Eisenhower.

The huge cost and complexity of this program, something the OSS could never have handled, was well worth it. Discoverer 14's single orbital mission produced broader surveillance coverage of the Soviet Union than every previous U-2 mission combined. By the summer of 1962, CORONA satellites were providing critical intelligence on Soviet and Chinese strategic infrastructure, exposing the fact that there were only a dozen Soviet launch sites, despite claims that there were more than 250.

The CORONA program was successful on a scale that changed the course of human history. Its satellites may have been the linchpin that averted nuclear war by letting knowledge and reason (rather than mystery and anxiety) govern decisions. The successors of Bissell's program at the CIA are now agencies in their own right: the National Reconnaissance

Office (NRO), which develops, launches, and manages satellites; and the National Geospatial-Intelligence Agency (NGA), my former employer, which tasks those satellites and analyzes their images.

The spy of the modern American imagination was also born during this time. James Bond, Jack Ryan, George Smiley, even Austin Powers—all these swashbucklers have roots in this moment in history. The Cold War was the time when new agencies were born, when money flowed freely, and when secrecy was tantamount. In many ways, it was a war waged by spies. It was a conflict fought against not only a powerful empire in the Soviet Union but also the most sophisticated and far-reaching intelligence agency and secret police ever created, the Komitet Gosudarstvennoy Bezopasnosti, better known to us as the KGB. The Soviet Union's security agency was a global professional organization that had honed its ruthless tactics through decades of secret police actions under Stalin. Our "glorious amateurs" were war heroes, sure, but U.S. intelligence needed to grow up and play hard in order to face this enemy. Indeed, the OSS had been thoroughly infiltrated by communist agents during the war, something that was unacceptable in the new paranoid reality.

The stakes were as high as or higher than during World War II. By the early days of the Cold War, the Soviet Union had the largest standing army in Europe, with three million active soldiers. The USSR was spending more than twice as much of its gross domestic product on defense as the United States. Given their focus on self-sufficiency, which was driven by a highly centralized government, and their focus on heavy industry, the Soviets were quickly modernizing and expanding both their army and their economy. On August 29, 1949, they tested their first atomic weapon, built from plans stolen from the U.S. program due to our poor counterintelligence, and in 1953, they tested their first hydrogen bomb, a weapon that could herald the end of the world.

With the writing on the Iron Curtain, in 1947 Congress passed the National Security Act. This legislation created the CIA and several other key national security organizations, including the U.S. Air Force, the Department of Defense (DoD), and the National Security Council (NSC). The CIA, unlike the OSS and the COI before it, was a permanent,

independent civilian institution with its own funding. While this new agency incorporated pieces of the OSS, it created its own culture, bureaucracy, and operational approach—one tailored for a new, very different enemy.

When President Dwight D. Eisenhower laid the cornerstone at CIA headquarters in the leafy suburb of McLean, Virginia, on November 3, 1959, he also laid to rest any doubts that the United States would return to the Stimson days of distaste for gentlemen reading one another's mail. By the time the headquarters building opened in 1961, it had 1.4 million square feet of office space on 258 acres. In Washington, having a headquarters of this size is a sign of permanence. Peacetime intelligence with global ambitions was here to stay.

The CIA would take the basic construct of the OSS and scale it to enormous proportions. The various OSS directorates (from operations to analysis to support) would remain and eventually expand to include several mission centers and other organizational constructs. The Cold War globalized the CIA and U.S. intelligence. Officers were posted around the world. Their remit was securing the United States in every way and against any threat, especially the central concern of the day, the communist menace. CIA officers also operated in what is known as non-official cover, by posing as businesspeople or other nongovernment positions. As with World War II, allies were key, and the CIA and other agencies set up information-sharing agreements with the United States' closest intelligence allies. The core of this secret alliance was in the English-speaking world of the British, Canadians, Australians, and New Zealanders—a group that would come to be called "Five Eyes," which was allowed see certain intelligence reports. Five Eyes remains an important alliance to this day.

Intelligence also became highly professionalized. The Farm, where I was trained, was established in southern Virginia. This is where case officers learn tradecraft, the term used to describe the specialized skills and processes of intelligence. CIA officers and, later, other agency officers were recruited secretly, rigorously selected, and trained to operate clandestinely anywhere in the world, under any conditions. Operations went from the OSS's fly-by-the-seat-of-your-pants cowboy plans to highly detailed,

massive, sometimes yearslong affairs run by tens if not hundreds or even thousands of people. Agency R&D went from Lambertsen's dive in the Shoreham pool to programs to create the multibillion-dollar U-2 and, later, the world's fastest airplane, the A-12 Oxcart. Satellite and other programs were not merely at the cutting edge of technology; they invented the cutting edge. Analysis morphed from the congenial and academic to a structured, highly analytical affair that continually produced an updated view of the world's threats delivered to the president every day in the form of the President's Daily Brief. In 1941, the OSS had an authorized budget of ten million dollars, whereas the single CIA Cold War operation Project Azorian, which attempted to raise the Soviet K-129 submarine, cost billions in today's dollars.

The CIA was not alone in its massive growth at the time. Over the following two decades, Congress authorized an entire suite of permanent peacetime agencies designed to collect and analyze different forms of intelligence, creating a series of so-called three-letter agencies to work alongside the existing military service intelligence offices in the Army, Navy, Air Force, and Marines. The National Security Agency (NSA) was formed in 1952 to perform signals intelligence. In 1961, the National Reconnaissance Office (NRO) was created to design, build, and operate space-based collection platforms. To provide strategic intelligence to the military, the Defense Intelligence Agency (DIA) was established in 1961.

Intelligence needs to know everything about the world to help decision makers. To keep it straight on how this happens, it helps to think of the intelligence apparatus as a person. To assess the world and decide what to do and how to behave within it, it needs senses. The Intelligence Community provides the various senses that help the larger organism determine how to act. Each sense is good at getting some types of information, but not others. Only by combining these senses can we get a full picture of the world. These days, every type of collection is given an intelligence, or "INT," name, and you can refer to these various collection methodologies as "the INTs."

Most modern electronic technology produces some form of signal, either on purpose, as a form of communication, or incidentally. The ears of

intelligence might be signals intelligence, or SIGINT, which collects information from electromagnetic signals from communications devices like radios and cellular phones, known as communications intelligence (COMINT), or from vehicles or other devices that create an electromagnetic signature, called electronic intelligence (ELINT). These might be cell phone calls, military radio communications, the telemetry data of missiles, or the leakage of any electromagnetic signal from a device. Knowing that all these signals are monitored, and that adversaries therefore encrypt them, the NSA also focuses on the encryption and decryption of these signals. For this, it maintains large cadres of code breakers and purportedly employs the most mathematicians in the world. More recently, cybersecurity—including the defense of government computer systems and offensive infiltration or sabotage of adversarial systems—has become a more significant portion of the work done by the NSA and its sister combatant command CYBERCOM.

To continue the analogy, the eyes are the geospatial intelligence, or GEOINT, which incorporates the analysis of images taken from space or aircraft, known as imagery intelligence (IMINT), with intelligence gained from maps or geospatial datasets into a complete GEOINT product. A GEOINT analyst might analyze a map alongside satellite images of road conditions to best determine routes for enemy vehicles, for instance. Think of these products as being like Google Maps, where you have all this data (e.g., the opening times of a restaurant) and images layered on a map. A GEOINT analyst might closely analyze a satellite image of an enemy installation to create a targeting package.

We might think of the taste, smell, and touch of the intelligence world as something called measurements and signature intelligence, or MASINT. The Office of the Director of National Intelligence defines MASINT as “an intelligence discipline built on capturing and measuring the intrinsic characteristics and components of an object or activity. These characteristics allow the object or activity to be detected, identified, or characterized every time it is encountered.” Multiple types of sensors can be used to take measurements that can then be used for MASINT analysis. For example, a sensor might be set up behind enemy lines to measure

distinctive features, such as acoustics, and then that information can be analyzed alongside other intelligence to tell when and where the enemy is moving. One might also measure the movement of water into and out of a house, to figure out how many people are in the house. This form of intelligence can take the shape of any object detectable by a sensing instrument, from acoustics and sonar to photography and radioactivity. If it sounds a little hard to grasp, that's because it is, and even within the Intelligence Community, there is debate as to exactly what MASINT is and isn't.

The oldest form of intelligence is human intelligence, or HUMINT, which is intelligence collected through the use of human sources. Typically, this is done by a case officer who will spot, assess, recruit, and manage intelligence sources. Unlike in the Hollywood imagination, most professional case officers do not actually collect the information themselves. That would not make much sense—why have an American from Idaho try to infiltrate the Taliban or the Chinese Communist Party, respectively full of Pashtuns and Han Chinese, when you can recruit someone from the Taliban or the CCP to do it for you? Doing this is extremely hard because, of course, the adversary does not want you to spot, assess, recruit, and handle its people, so it institutes counterintelligence at every turn to stop you. Because of that, case officers use a series of specialized techniques to do their jobs.

These are the classified INTs, the ones that use secret technologies or processes to get information, but there is also all the publicly available information in the world. This is what the Intelligence Community calls open-source intelligence, or OSINT (or what everyone else outside intelligence just calls "getting information"). OSINT includes collecting all the other information in the world that can be collected to inform intelligence, from newspapers to social media to scientific articles to technical manuals. Even the Moscow phone book was once considered a collection requirement. For a long time, this sort of information has been considered a second-class citizen in intelligence. It is necessary for analysis but is also the sort of thing the new guy might be expected to work on. At the same time, OSINT is suspect because its openness makes it ripe for

manipulation. But as more and more information and data have become available on the internet, OSINT has grown in importance.

★ ★ ★

The Cold War golden age of intelligence also made intelligence secret. Of course, the OSS tried to be secret about what it was doing, but it was a wink-wink, nudge-nudge secrecy with little significant counterintelligence. More sinisterly, the OSS was infiltrated by communists, and many secrets were leaked back to the Soviets. While that might be okay in the fast-and-loose era of a world war, it could not stand during the Cold War, when secrecy was necessary to keep the war from turning hot. The CIA and, later, other agencies implemented intense counterintelligence and created the system of classification and compartmentalization that today marks the world of intelligence.

Secrecy and classification set apart intelligence from information and intelligence officers from the rest of society. Intelligence is like knowledge in a secret society. It is something that is controlled and hierarchical, available only to the initiated. It is a treasure that is contained by and constrained within a hierarchy of classification. There are levels of knowledge. Some people have access to certain knowledge, and others don't. In the Freemasons, you might gain new knowledge as you move up the ladder from an Entered Apprentice to a Master Mason. In intelligence, you are granted access to information only after you are granted a security clearance and have "a need to know."

There is the old, somewhat trite saying that knowledge is power. In the world of intelligence, that can literally be the case, because in that world, certain information can cause damage, death, and destruction. Even the term *classification* is legally defined around the concept of damage. It is explicitly defined like this: Confidential information would cause "damage"; Secret information, "serious damage"; and Top Secret, "exceptionally grave damage." Given the different levels of damage, at each level, you need more and more protection.

The apex of the pyramid, Top Secret, is the world in which intelligence officers operate. At the Top Secret level, intelligence officers work and

operate within SCIFs, “sensitive compartmented information facilities.” These are physically secure, specially constructed rooms and buildings protected by guards and technical means to hold classified information. There is a labyrinth of security to get into and out of an SCIF, starting with a badge designating your permission to be inside. The badge itself sets you apart from others—for example, blue designates you as a government employee, green as a contractor. Unlike your work badge, security badges have no names on them, protecting the identities of those wearing them. Often that labyrinth leads to a windowless room with few people in it, where even peeking over a shoulder to see what is on a monitor in the next cubicle over is forbidden. If you work in a Top Secret environment, as I did for quite a while, you might spend hours or even your full day inside a windowless room, with no access to a cell phone or other outside communication. You are completely cut off from the real world, your only feed into what’s going on being classified intelligence and perhaps a news channel on a television in a break room.

Many more people operate at lower levels of the pyramid. Generally, most of the military operates at the “Secret” level. This is, in some ways, a practical matter: they need less security for Secret information, and SCIFs are hard to come by on the battlefield. “Confidential” information is less common and used for the lowest level of security. The government also has its own version of proprietary information, “Controlled Unclassified Information”—similar to when you mark a document at work as confidential to your company. This information is not classified per se, but it should be protected, and it should not be shared.

Contrary to what the books and movies say, there is no “above Top Secret.” Rather, what happens next is that the information becomes compartmented. A person with classification authority designates a piece of information as “sensitive compartmented information” and can grant special access to those compartments. There is then what is called a Top Secret/SCI clearance—or, as you might more often hear it, TS/SCI. Some compartments can be broad, meaning most people at an agency have them. At the NGA, for instance, most people have access to at least some satellite imagery compartments. There are also narrower, highly specific, and highly

secret “Controlled Access Programs” (CAP) or “Special Access Programs” (SAP). These are usually about a single operation or weapon system or some other secret activity to which only a few people have access.

Compartments are the way into the deepest recesses of the Kafkaesque world of intelligence. To be “read on”—to use intelligence officer slang for gaining access to a compartment—means that you are given an additional nondisclosure agreement that lets you see this new compartment and then given a brief on generally what is included in that compartment. Reading people on also allows agencies to keep track of who has access to what compartments and ensures that only those with a need to know are allowed to see the information. But it is more than that.

To be at the heart of the secrecy labyrinth is to know something that no one else around you, maybe no one else in the entire building, knows. Now you are keeping secrets from the other badge-wearing initiated around you, perhaps something so secret that it cannot be emailed, even on a classified system, but must be hand-delivered. Some secrets must be protected more rigorously. But this level of security can also lead to absurdity. Take, for example, formerly read-on people being “read off,” meaning they have to sign paperwork saying they no longer know that information and can’t access it. So you may be in a situation in which you know something but aren’t allowed to talk about it, even though you and the person you are talking to both know that you know about it. Imagine working on a project every day for a decade with your friends and then, all of a sudden, not being able ever to talk to them about it again, in public or private.

Worse still, secrets in the world of intelligence are weaponized against not only the enemy but also one’s own side. Within the IC, culturally it is a sign that something is neither important nor even true if it is not marked as “Top Secret”; or nefariously, something can be arbitrarily defined as truer if it is designated as such. Also, people actively make information *seem* more important than it actually is through classification. Classification is also used as a means of bureaucratic competition. If someone has classification authority—such as if the program or operation belongs to them—they can designate it as an “SAP/CAP” compartment. They then get to choose who is read on to that program. Conversely, they might also ensure that certain

people are not read on. While there might be great security reasons for such a decision, there might also be ridiculous or personal or even dangerous reasons—for instance, you don't want another agency to know what you are doing. That is, maybe you are doing a mission that arguably should be theirs, or you just don't want anyone else to know about a certain activity because they might critique it or threaten your budget. Welcome to the world of intelligence bureaucratic politics.

As with the Freemasons, access to information is granted only to the initiated. But instead of a mystical ritual, access in intelligence requires a security clearance. Like Catholic confession, a security clearance requires you to confess all your sins. You do this in a seemingly endless form, the SF-86. The government must know everything: every foreigner you've met, every place you've lived, every drug you've done, every job you've had. And unlike your neighborhood priest, the government will trust, but verify: counterintelligence officers will visit your friends, neighbors, and employers to ensure that what you've said is true. But the paranoia does not stop there. Next comes a polygraph, where you're hooked up to wires that measure your physiological responses and again asked to confess.

The counterintelligence search is exhaustive and often embarrassing, but necessary. The point is to make sure you are a trustworthy person and that there are no easy ways to blackmail you for information. Once granted a clearance, you must begin to follow the rules of your order, to continue the metaphor, reporting whenever you break the law, obtaining permission to travel abroad, and having anything you intend to publish reviewed. (This was so for the book you are reading, which was reviewed and approved by agency personnel.)

The ironic eye-opener is that once you receive a clearance, you will find that most classified information is pretty boring. As I did upon receiving my clearance, you might imagine all the secrets being revealed to you—from the existence of space aliens to JFK assassination conspiracies to the location of the Holy Grail. Instead, what you will find is more like an extension of what is available in the unclassified world. If you studied international relations in college or even just have a strong interest in it, you'll be pleased to find you can access vast amounts of information on

foreign countries and their leaders, analyses of their intentions, and so forth. You can even research which weapon systems their armies have and what sort of satellites they've launched. Classified information mainly adds a layer of detail to what's publicly available. There is more analysis and insight available to those with clearance, though it's not light-years better than what you'd find online or in a library. On the military front, you might have some more technical stats on an adversary country's tanks or fighter jets—say, the specific frequency at which its radar operates—but 99 percent of the time, the additional detail isn't particularly mind-blowing to all but the most trained.

But if you are a nerd like me, you may find it fascinating. You may crave knowing as much as you can about a particular country or how a leader thinks. Or maybe you are an aerospace fanatic and you want to know as much as you can about various aircraft, their capabilities, and how they're made. And frankly, this is the reason many people become intelligence officers. Choosing this path indicates a kind of curiosity about the world, especially the parts of it that interest you. And, well, if you like that kind of thing, you should sign up.

Yet the smallest sliver of competitive advantage gained from classified information is often the most important game changer. Knowing slightly more about how radar works can be the difference between making a decision that leads to mission success or being shot out of the sky by enemy missiles. A president or secretary of state needs all the information they can obtain to make tough calls on international negotiations. It is this competitive edge that drives the entire intelligence apparatus, and it is because of the importance of this edge that information must be controlled and protected.

★ ★ ★

The golden age of intelligence is still very much with us. The agencies, the INTs, the classification, the global footprint and operations, the training, and, more important, the culture—all these are the baselines of U.S. intelligence upon which everything else is formed. They are also for me,

personally, the baselines of my own intelligence training, even though I was still in elementary school when the Berlin Wall fell.

Much of the training I received at the Farm was very much in keeping with the old-school-style training that Cold War officers received. In fact, when I showed up for training, it felt like I had landed on a campus preserved in the idyllic past, complete with rolling hills, whitetail deer roaming freely, and, surreally, bicycles that could be swapped out and ridden from meeting to meeting. But I wasn't there to take anything resembling a freshman seminar. Instead, I had arrived to undertake the most rigorous training course in the Intelligence Community, one that Navy SEALs and PhDs regularly flunk. This ferociously intense and mentally exhausting series of exercises was intended to teach us prospective agents how to find, assess, and handle intelligence sources. The lessons I learned were distilled from decades of CIA operations since the agency was established in 1947.

Most of my instructors at the Farm learned to operate in the Cold War environment, where operational security and counterintelligence were vital. They were up against the best internal intelligence service in the world, the KGB. The stakes were high—nuclear war, if things went really badly.

The Farm is the pinnacle of the golden age of intelligence. It distills all the lessons learned and spares no expense in creating generation after generation of highly trained officers. Students learn to detect surveillance, to develop a source over time by building trust, and to communicate with and otherwise handle sources securely. One day, this might mean finding a good dead drop location, where you can secretly hide a message or item. Another day, you might have to memorize a complex communication plan and teach it to a difficult source. Or you might have to stand up to interrogation in a mock scenario while remembering your cover story. This is the real stuff of espionage. It's all primarily learned by role playing. Imagine playing a monthslong game where you are pretending to be a spy and where role-playing instructors are both mentoring you as you go and also figuring out whether you are going to be any good at it.

It's not just the Farm that was special; the entire U.S. intelligence system was perfected to fight a global intelligence competition during the

Cold War. For five decades, the U.S. Intelligence Community pushed forward with its golden age–born ethos of unrelenting innovation and information gathering. It was at the top of its game. Until this highly optimized apparatus broke. And when it did, the results were catastrophic.

OceanofPDF.com

3

The Chaotic Age

In 2008, not long after graduating from the Farm, I was shipped off to Baghdad. Like many around me, I signed up after 9/11 to get in the game, and into the game I went. Operations in Iraq were a far cry from the days of working out of a Cold War embassy. Our days began with a 6 a.m. security briefing (often with an episode of the oddly soothing show *How It's Made* playing in the background), in which we would go through the previous day's insurgent activity and the forecasts for the day. Sort of like a weather report, but for improvised explosive devices and ambushes. We plotted out our routes through Baghdad carefully, incorporating information about potential military operations into our plans. Because operating alone in Baghdad was essentially suicidal, we worked in teams, with soldiers to protect us and interpreters to help with the language barrier.

One of the sounds I can recall most distinctly and that instantly brings me back to Iraq is the metallic zing of a steel magazine being loaded into a rifle. That is not what intelligence normally sounds like. It's usually a quiet affair involving walking inconspicuously down side streets, holding low-volume conversations in restaurants, and hearing the occasional squeak of chalk as you leave a signal on a brick wall. The job is to get intelligence and to ensure that you and your asset remain safe. The same thing taught at the Farm, just in a new place.

Inconspicuousness, being the "gray man"—someone who dresses, talks, and acts so as to not be noticed—is the true bulletproof vest of the intelligence officer. The same applied in Iraq. Perhaps we could fight our way out of a checkpoint gone wrong, but better never to be noticed in the

first place. It's best to blend in, looking like a local as much as possible. This is a lesson taught to all spies since time immemorial. As is observation, noticing everything, whether it is an odd-looking fellow on a street corner who might be a surveillant or alarming trash on a street that could be an IED. To this day, it's hard for me to run over litter or anything lying in the street, and the sound of someone walking up behind me can raise the hair on the back of my neck.

Regardless of the threats, intelligence still needs to be collected. Indeed, the greater the threat, the more we need the intelligence. And this is the most lasting lesson I took away from the Farm. It is not about not taking risk; rather, it is about taking *calculated* risk. Sometimes, that calculation may require lots of physical risk to get something done—and the real threat of death for you or your source. Sure, you could stay in the relatively secure Green Zone all day, but then how would you ever get good intel and help win a war?

After the attacks of September 11, 2001, a return to a pre–Cold War ethos of taking bigger, or at least more immediate, risks was necessary for the Intelligence Community, a change that has affected an entire generation of intelligence officers like me. Our first experience in intelligence involved guns, murdered sources, and roadside bombs. This calibrated us in a completely different way from the Cold War warriors we followed—when it came not just to working in a war zone, but also to considering all forms of covert and clandestine action and adopting new technology and new ways of doing intelligence. This return to risk-taking was necessary for what happened after 9/11.

★ ★ ★

The disastrous events of 9/11 were an intelligence failure that thrust the United States into the next revolution in intelligence. As *The 9/11 Commission Report* showed, U.S. intelligence and law enforcement agencies had pieces of the puzzle of the 9/11 hijackers' plans, but they did not connect the dots. The compartmentalization of intelligence between and within agencies meant that the right information was not shared with the right people at the right time. A new, decentralized enemy like Al-Qaeda or

ISIS could then slip through the cracks between domestic and international, the CIA and the FBI, counterterrorism analysts and counterintelligence analysts.

The perfectly optimized Intelligence Community, made to fight a global, centralized, counterintelligence-focused adversary like the Soviet Union, harmed itself. It was almost like an autoimmune disease. U.S. intelligence was actually too good at the job it had done over the previous five decades and not at all ready for the one at hand. As before, a new enemy and new technology, for which agencies were not adapted, would transform intelligence.

Fighting a dispersed global threat required a new form of intelligence. Suddenly, the military knew it had to "find, fix, and finish" terrorist threats —a euphemism for locating an enemy fighter somewhere in the world, keeping track of their location long enough for forces to establish contact, and then either capturing or killing them. We also had to figure out how to close the gaps and connect the dots in an increasingly complicated world where technology was networking and globalizing everything.

In response, U.S. intelligence adopted three major new approaches to intelligence. One was the return of intelligence to war, in both Iraq and Afghanistan, but also, in covert actions globally. The second was the adoption of new technology to create network intelligence. Third was the integration of intelligence and other agencies into what came to be called a whole-of-government approach.

The war against Al-Qaeda and other terrorist groups required a global footprint, as in the Cold War, but with more direct tactics. Decentralized terrorist groups crossed borders without regard to international convention; they operated wherever they could. The IC leaned into that mission to help find and fix targets; that meant we had to go wherever they were. More often than not, this meant leaving the embassies and other safe havens and going into the streets of Sadr City, Baghdad, or the caves of Nangarhar Province, Afghanistan. U.S. intelligence officers had served in every war, publicly and not so publicly, throughout the Cold War, but they had not mobilized such huge numbers to deploy to war zones since the days of the OSS.

Clandestine intelligence (when you keep your actions secret) is not the only mission of intelligence agencies. Covert action is the other mandated mission of intelligence agencies like the CIA. Being covert does not necessarily mean being secret. Rather, being covert means the identities of both the mission and its operators are concealed or at least plausibly deniable, but the action itself may be known. A covert action could be something like an influence campaign, or it might involve the training of local militias to combat a regime, or it could be the killing of a particular terrorist. The special authority to undertake covert action was codified in the National Security Act of 1947 as a specific directive of the CIA, though the president may opt to have other agencies take part, or the CIA may partner with other agencies. Either political or paramilitary in nature, covert action requires a "presidential finding"—which is a formal directive and notification to the appropriate congressional committees—and since 1991, it has required oversight by special committees in the House and Senate.

During the war on terror, covert action was used for exactly what you might imagine it was. Terrorists were located somewhere in the world, found, kept in sight, and then finished. That final euphemism can mean many things. One meaning might involve extraordinary rendition, which is when someone is captured, transferred out of the country, and imprisoned. Another meaning might involve the use of drones like the MQ-1 Predator or the MQ-9 Reaper, with Hellfire missiles to kill the target—sometimes referred to as a "targeted killing."

Both these activities, extraordinary rendition and targeted killing, were highly controversial and remain so. From the intelligence officer side, they are generally considered legal and necessary for defending the nation from another attack—though there has been debate also within the Intelligence Community about the practices. For me, this is another area where the American population needs to know what is going on and have a knowledgeable opinion on it, because as an electorate, they do have a say. Laws and policies govern intelligence operations, including covert action. Voters elect the officials, from presidents to Senate and House intelligence committee members, who determine those laws and policies. In a democratic nation, we can make up our minds about whether something is

ethical—or about whether we are willing to live with an ethical stain in exchange for more security—and we then have a say as to whether we want our leaders to do that thing. The situation is made more complex because covert action is, by its nature, secret, and voters must make their wishes known either through selecting for the character of their leaders or making their ethical line known publicly so that those already in office know not to cross it. Regardless of where you stand on the issue, knowing about intelligence and covert action, paying attention and having a say, matters now as much as it did during the war on terror.

Accomplishing the intelligence and covert action missions against highly decentralized enemies required new technologies. Throughout the Cold War, the government drove most R&D in the United States, but around the mid-1980s, the commercial industry took the lead. By the time of the first dot-com boom, in the late 1990s, it became clear that Silicon Valley was now driving technology innovation. If it were to stay on the cutting edge, the Intelligence Community would therefore need to turn to innovative tech companies.

In a prescient move, CIA Director George Tenet ordered the creation of In-Q-Tel, which in 1999 became the CIA's very public venture capital company. Organized as a nonprofit, with its own sole-source contract with the CIA, it would partner with other venture capital investors, like the capital market company Andreessen Horowitz, to find technologies that might be valuable to the Intelligence Community and invest in them. For example, Keyhole, a satellite imagery software company, received early funding from In-Q-Tel on behalf of the National Imagery and Mapping Agency (NIMA), one of the precursors to the NGA. That investment enabled NIMA to use Keyhole's technology to assist in its national security mission. Keyhole would later go on to be acquired by Google and form the nucleus of what would become Google Earth and, later, Google Maps. Another In-Q-Tel company, Palantir, would become a key player in providing social network analysis in the Global War on Terror and, later, go public in a groundbreaking IPO.

After 9/11, the Intelligence Community needed to revolutionize its technology into what can be called network intelligence. Agencies had to

find new ways to acquire all the data now available in a connected world, in ways less like installing individual phone taps and more like getting access to all the calls and data transmission from the telecom network provider itself. Once the agencies had the data, they needed to then use new network analysis tools, such as the software that Palantir and other companies made, to sift through and make sense of it. These developments led to the expansion of a whole arm of intelligence, called targeting. The practitioner of this, called a targeting officer or targeter, specializes in using technology to find people with networked data.

The single biggest revolution in intelligence that arose out of 9/11 was the wholesale reorganization of the agency structure into the Intelligence Community. As the National Commission on Terrorist Attacks Upon the United States—also known as the 9/11 Commission—found in its hearings, the FBI and the CIA had pursued separate investigations into various members of the Al-Qaeda terrorist organization and, problematically, had not shared this information with each other. This, the commission explained, enabled the success of the attacks. In other words, the compartmentalization that the Cold War had perfected to protect secret operations was now the problem.

Back in October 2000, suicide bombers blew up the USS *Cole*, which had stopped in Yemen to refuel. The attack killed seventeen U.S. sailors and injured many more. During its investigation into the bombing, the FBI zeroed in on a suspected mastermind, an operative known as Khallad, also known as Walid bin Attash, who was a bodyguard to Osama bin Laden. (Khallad's nickname was "the Father of the Leg" because he wore a prosthesis after losing a leg in a battle with Northern Alliance fighters in 1997, an experience that led him to join Al-Qaeda.) The CIA, investigating a meeting of Al-Qaeda agents in Malaysia at which Khallad was present, did not sit down with FBI investigators until eight months after the *Cole* attack. The meeting in Malaysia, which intelligence officials now believe was held to plan both the attack on the USS *Cole* and the attacks of 9/11, revealed a lack of long-term coordination and produced further acrimony between the two agencies.

In another episode, Khalid al-Mihdhar, a twenty-six-year-old Saudi and one of the 9/11 hijackers, who was also present at the aforementioned Malaysia meeting, had been issued a visa to enter the United States. The CIA claimed it sent an email with this information to the FBI, but FBI records indicated that no such message was received. The CIA also admitted that it did not inform any department that al-Mihdhar had gone to Los Angeles, and it did not approach the State Department about placing the men from the meeting on a terrorism watch list. In late August 2001, just weeks before 9/11, the CIA requested that the FBI help track down two of the eventual 9/11 hijackers, a request that was denied by FBI headquarters. The list of missteps and lost opportunities goes on.

The 9/11 Commission was resolute. Keeping law enforcement separate from intelligence was detrimental to national security and had led to gaps in U.S. intelligence that enemies could exploit. The cloistered Intelligence Community needed to be further integrated into the wider system of government. This finding led to the biggest change for U.S. intelligence in this post-9/11 moment: the move toward a whole-of-government approach.

Since then, the IC has made numerous organizational changes to connect law enforcement and intelligence and has ensured that other government agencies are brought into the loop to make counterterrorism efforts more effective. For example, a National Counterterrorism Center (NCTC) was created to allow the various agencies to literally sit down together to share information and authorities in order to pursue a singular mission, stopping terrorist attacks. Additionally, the Intelligence Community had to bring many new agencies into the fold. For example, because many terrorist plots involve transport, such as hijacking airplanes or bombing trains, the Department of Transportation became more closely involved with the IC. By sharing authorities, such as domestic law enforcement by the FBI with foreign intelligence collection by the CIA, the NCTC could connect all the dots and, it was hoped, stop the next attack.

Most impactfully, the 9/11 Commission recommended adding a director of national intelligence (DNI) as a cabinet-level position. Before 9/11, the director of central intelligence (DCI) had three separate jobs: managing the CIA, organizing the entirety of the IC, and working as the

president's chief intelligence adviser. While such a role may have worked during the Cold War, the DCI position became untenable as the IC expanded. The CIA is one agency among many, and having it as the integrating authority was not working.

The creation of the cabinet-level Office of the Director of National Intelligence (ODNI) by President George W. Bush meant one entity could have objective oversight of all members of the Intelligence Community. The ODNI oversees a much wider set of organizations beyond just the big five agencies (CIA, DIA, NGA, NRO, NSA), including Army, Navy, Air Force, Marines, Space Force, and Coast Guard intelligence; the Departments of Energy, Homeland Security, State, and Treasury; the Drug Enforcement Agency; and the Federal Bureau of Investigation.

Lastly, the counterterrorism mission further expanded the Intelligence Community internationally. While Five Eyes continued to be the centerpiece of intelligence sharing, other alliances like NATO have been added to intelligence-sharing agreements; or if those agreements already existed, they were expanded and strengthened. Meanwhile, the scope of this intelligence sharing increased after 9/11 to include some unlikely allies. In 2010, Saudi Arabia received information on an Al-Qaeda plot to attack cargo planes headed to the United States. Saudi officials alerted British, U.S., German, and Emirati intelligence officers, who were able to organize and prevent the attack. In 2017, the CIA even warned its Russian counterpart, our longtime Cold War enemy, of a plot by a terrorist cell in Russia looking to bomb various sites around St. Petersburg. This international expansion continued a general trend of intelligence becoming broader and broader, reaching into more and more corners of the globe and society.

★ ★ ★

Since the beginning of World War II, the IC went through three great transformations in response to profound new geopolitical challenges. It expanded its operations into more and more corners of the globe. Responding to each new threat required new organizations, new missions, and new approaches to intelligence tradecraft. Each of these three

transformations saw resulting advances in technology: first, we had Nazis and radios; then Soviets and satellites; then Al-Qaeda and the internet. Each transformation also expanded the range of who did intelligence, from one agency and the military, to many agencies, to the whole of government.

During this time, the intelligence mission remained the same. The bread and butter of intelligence still involved understanding things like the internal machinations of the Kremlin or whether there might be a coup in a West African nation. Agencies would write up a psychological analysis of a terrorist leader, making predictions about where he might next order a bombing; tally the military equipment and personnel in an adversary's military; obtain a MiG fighter and find out how its radar worked; and assess the probability of whether Russia would invade Crimea or was just bluffing —typical national security intelligence for much of the past eight decades. This intelligence is necessary for U.S. diplomatic relations and military decision making. Presidents and national security advisers and generals need this information every day. We have been doing this since the days of the OSS, and we are quite good at it. This is our comfort zone.

This type of intelligence, in its several forms—political intelligence, military intelligence, indications and warning, and intelligence liaison—remains necessary. Political intelligence is what many people think of when they think of spies. The president needs to know what foreign leader is most likely to cause a disturbance, or whom the National Security Council needs to assess as the next potential head of state in a country with whom we have an important relationship. Political intelligence is the domain of the case officer stationed at an embassy, who clandestinely meets with and then recruits someone in the Ministry of Foreign Affairs to secretly collect information. It is the type of intelligence done by someone listening in on a foreign minister's phone conversation to overhear the contents of sensitive meetings.

Military intelligence includes things like finding out the order of battle of foreign militaries—meaning, the organization, equipment, personnel, and strength of other countries' armed forces. When defending the United States, the Pentagon needs to know what to prepare for. Defense attachés, the military officers stationed at embassies, interface with their counterparts

and collect public information as they watch military parades or take tours of bases. Satellites spy on air bases, and analysts count the number of fighter jets on runways. HUMINT sources sneak out the plans for the latest submarine.

A hugely important intelligence mission is indications and warning, or I&W. This is the mission, as its name implies, to find and report timely warnings about the intents or actions of adversaries. It might be when an agency tracks and monitors the cell phones of terrorists to see whether they might attack Americans, or when it brings together satellite information and spies in the Kremlin to see whether or when Russia might try to invade Ukraine. The more time for a warning, the better because it buys time and space for decisions to be made. This mission is also the one we most often associate with an intelligence failure, such as with Pearl Harbor or 9/11.

Another mission that many don't often consider is intelligence liaison, including intelligence sharing. One of the roles of intelligence officers is to work with other intelligence agencies around the world. There are intelligence alliances just as there are military alliances. In the Five Eyes alliance, for example, the aligned nations share signals and other intelligence-collection capabilities, data, and analysis. Such intelligence sharing and alliances are carried out by intelligence officers, just as a State Department Foreign Service officer might interface with a foreign government on civil issues or a military officer might work with NATO allies.

In the fourth intelligence revolution, we will continue these missions, though using different technologies and processes. At the same time, there will also be new missions and missions that were minor in previous eras that will become much more significant. The fourth intelligence revolution thereby demands the expansion of how we think about and where we source our intelligence. Intelligence will be applied to an ever-widening range of domains: land, sea, and air; outer space; cyberspace; our minds; and even our genetic codes. We must consider not only the political and military but also the economic, cognitive, and biological realms. These are the new intelligence battlefields.

Missions in the fourth intelligence revolution are driven by our adversaries' use of asymmetry to threaten us. Adversaries consider all the gaps and weaknesses at every place in our government, economy, and society and attack us with methods outside the traditional, straightforward, or expected approach. It is like how Al-Qaeda was able to slip through the cracks between the CIA and the FBI. Not all attacks will be political or military in nature. Our enemies will try to find and exploit every potential weakness, every chink in our armor. Doing this makes all areas of society, economics, and science part of national security. By securitizing these domains (i.e., making them areas of national security importance), we must in turn come to defend those areas as well, just as we came to defend the political and military domains.

Understanding how the fourth intelligence revolution will expand the scope of intelligence requires understanding our adversaries. Authoritarian adversaries, particularly China, and the threats they present are the biggest drivers of the intelligence revolution. These enemies have their own unique ways of operating, and intelligence must adapt to them. The way such adversaries have adapted to challenging the United States has caused the world of intelligence to change drastically. The resulting transformation is fundamental and includes who conducts intelligence, how it is done, where it is done, and with what tools it is done. Countering our adversaries will require the greatest and most fundamental transformation the IC has ever undertaken.

OceanofPDF.com

4

Asymmetric Adversaries

It was midnight, and the sun was shining in Olgino. This was one of the poshest neighborhoods of St. Petersburg, Russia, a city far enough north that in the summer, the sun barely sets. In a beige four-story building on Savushkina Street, a group of coders and programmers clacked away at their work at the innocuously named Internet Research Agency (IRA). The IRA had attracted them by billing itself as a cool tech company with a modern office, free lunches, and the feeling of opportunity. Inside, employees sported the universal urban-tech style, what you'd see on people lounging at a Blue Bottle Coffee or craning over a laptop at a WeWork cubicle in many U.S. cities.

From all outward appearances, IRA employees had the mundane job of writing reviews and other related Web content. They had a quota, for instance, writing one hundred comments per day on social feeds. The environment was more textile factory than Madison Avenue marketing firm, the goal being to produce as much quantity as possible as regularly as possible. Sometimes the work was a little more sophisticated, like writing blog posts or coming up with political cartoons.

While there are thousands of these types of troll companies around the world populating the internet with the endless streams of text we see every day in Amazon reviews, YouTube comments, or clickbait ads, this one was different. As one employee of the IRA told the *Washington Post*, when he arrived, he "immediately felt like a character in the book '1984' by George Orwell—a place where you have to write that white is black and black is white. Your first feeling, when you ended up there, was that you were in

some kind of factory that turned lying, telling untruths, into an industrial assembly line." In fact, the IRA wasn't writing overblown five-star reviews of hair dryers and kitchen appliances; it was creating disinformation to target Russia's enemies, both foreign and domestic.

The IRA was created and owned by Yevgeny Prigozhin, who was, at one time, one of Vladimir Putin's trusted lieutenants. The bald, bulldog-faced Prigozhin looked perfectly the part of a B-movie Russian Mafia boss, and his personal story was befitting one as well. After doing nine years in a Soviet prison for robbery and other assorted crimes, he set up a hot dog stand in St. Petersburg. With the fall of the Soviet Union and the rise of capitalism, he got into the grocery, gambling, and then restaurant businesses. For a time, at one of his restaurants, you could find Vladimir Putin dining next to George W. Bush.

In 2014, Prigozhin formed the private military company the Wagner Group, which would ultimately be his undoing. The Wagner Group was like Blackwater, but on steroids. It employed former soldiers and a smattering of criminals as mercenaries to fight Russia's covert and overt battles in Syria, Africa, and Ukraine. Prigozhin would later be assassinated for leading a Wagner Group–led rebellion against Russia's leadership. However, a less-well-known story is that one of his most impactful creations was the IRA, which he claimed to have thought up and founded in 2013.

IRA employees, who would come to be known as the Trolls of Olgino, created content that explicitly pushed the Kremlin's views. For the domestic audience, the trolls might write about how sanctions were not harming Russia but, in fact, making it stronger—black is white. But it was in their posts and content directed at Americans where they really excelled. They created a series of politically focused comments, posts, pictures, and videos that they planted in Facebook, Reddit, Tumblr, and other online social media platforms in the United States to sow distrust in the U.S. government, create and deepen divisions within the country around discussions of politics, and place doubt in the U.S. electoral system. Their goal, it appears, was to push American society to extremes on both ends of the political spectrum. As the Department of Justice dryly put it in its indictment, "Defendant ORGANIZATION [the IRA] had a strategic goal to sow

discord in the U.S. political system, including the 2016 U.S. presidential election. Defendants posted derogatory information about a number of candidates, and by early to mid-2016, Defendants' operations included supporting the presidential campaign of then-candidate Donald J. Trump ('Trump Campaign') and disparaging Hillary Clinton."

While thugs and autocrats may have ultimately been behind this attack on democracy, the day-to-day pawns were a bunch of twenty- and thirty-something Moscow techies and marketing people in jeans and sweatshirts, trading memes and texting back and forth about what to order for lunch that day. These were not sexy, Hollywood-style intelligence officers, men and women of intrigue sporting dark suits and stern expressions, moving swiftly through a giant ops center. They were the same type of young people who might have been working at an advertising firm in New York or an online marketing company in San Jose. The philosopher of totalitarianism Hannah Arendt talked about the "banality of evil" with regard to the Nazis. But to use that expression for the Trolls of Oligino would be giving them too much credit. This was the inanity of evil.

Among the astounding facts about the IRA is how little it all cost. Using an estimated one hundred thousand dollars in advertising, the IRA was able to post thousands of messages on Facebook and, ultimately, reach millions of Americans. Some additional money was spent on other platforms, and of course they needed to pay their trolls, who might make around seven hundred dollars a month. But even putting this all together, with something in the range of a few million dollars, the IRA was able to organize one of the most impactful covert influence campaigns in history, cast doubt on a foreign election, and thereby threaten the very basis of U.S. democracy.

How could something so inexpensive be so impactful? For one thing, the infrastructure for this operation (and many others that mimic it) had already been built by multibillion-dollar companies. It was just waiting there for someone to figure out how to use it for a purpose other than for what it was originally intended. In the same way, Al-Qaeda didn't have to build missiles to blow up buildings; they just needed to train a couple of pilots to fly already-built airplanes into their targets. This is an example of

asymmetric competition—a special one, what I'd call parasitical asymmetry: using the tools built by our own society against us.

Like a parasite, the IRA hitched a ride on the American technology complex. Facebook and other social media data were easily available for sale to those willing to buy it. This was entirely legal. In fact, it is still possible. If you wanted to buy the political preference data of several million Americans right now, you could do so. You could then try to influence those millions. It might cost around twenty-five or thirty cents for each click or "like" on Facebook and two or three dollars for a thousand impressions, which is when someone sees an ad. In fact, you could go right now and set up your own political or other ad within minutes. The IRA also used the analytics services of Facebook and its partner sites not only to post ads but also to learn more about, in a very sophisticated and targeted way, the audience it was going after. It could target groups by geography, demographics, and other factors to find just the right niche of right-leaning, white, religious autoworkers or left-leaning, Black, urban-dwelling activists.

Facebook and every other social media company had built these systems to allow advertisers to access their product. And what was that "product"? Us, all of us—our minds, our opinions, and therefore our actions, whether to buy or to vote. There is a saying: "If you are not paying for the product, then *you* are the product." To a social media company, the users on its platform are the product being sold. Social media was and still is offered largely for free for this reason, and so the vulnerability remains.

Given the level of detail that people willingly share about themselves on these platforms, it is possible to target very specific groups of people. For example, it's possible to target men aged eighteen to twenty-four who like pickup trucks and live in certain counties within Oklahoma. The companies have tools to help optimize ads to attract these particular people. This same targeting is being applied not just to consumer preferences but also to political preferences.

Like a Silicon Valley tech company, the IRA used consumer data and start-up approaches like the "lean start-up" method and A/B testing to figure out the best way to market its product. Lean start-up is a method for

building tech companies co-created by Steve Blank, an entrepreneur and brilliant thinker on technology (and national security), and his former student author Eric Ries. Using it, companies begin by offering a "minimum viable product," which is a version of a product that has the bare minimum of features necessary to launch into the market. They market that product and see what consumers think, and then update the product to better fit what consumers want. Companies can potentially change how it is marketed for some consumers (A group) as opposed to others (B group), to see which gets better results. A key component of the lean start-up method is to quickly pivot to a different business model, product, or marketing approach depending on what does best with consumers. The IRA was essentially doing the same thing. It obtained Facebook consumer data, built disinformation packages, and then offered up those packages to see which created the effect it was looking for.

There was no scientific or strategic analysis—as might have happened in the old days. Instead, they threw stuff at the wall and saw what stuck. If it didn't work, they moved on. If it worked, they went with it. It was basically a Russian covert influence operation taking a page from the book of Silicon Valley tech start-ups.

This is an example of a Russian intelligence revolution in action. The Russian path was very different from ours, as the Russian state had different objectives. The KGB was founded in 1954 to centralize foreign and domestic intelligence and had several other functions, like protection of the Central Committee of the Communist Party and counterintelligence in the Soviet Union. But with the fall of the USSR in the 1990s came chaos and a devastating loss of resources for state security. The KGB was broken apart into the internally focused Federal Security Service, or FSB, and the externally focused Foreign Intelligence Service, or SVR. Both were joined by the much larger Main Directorate of the General Staff of the Armed Forces of the Russian Federation, or GRU, the intelligence and special operations directorate of the Russian military. With many fewer resources at hand, Russia's intelligence agencies needed to find a new advantage, one where they could attack U.S. weaknesses with their strength.

One of the primary means by which the Russian intelligence services have regained their mojo is the use of active measures. Active measures involve using propaganda, disinformation, sabotage, assassinations, and other dirty tricks clandestinely or covertly to harm adversaries. Most intelligence agencies, including the CIA, employ covert operations to some degree, but the Russians really excel at their creative, ruthless use. Some public examples include creating rumors about HIV having been developed by the U.S. Army in Fort Detrick in the 1980s, organizing and backing world peace protests against U.S. deployment of nuclear weapons in western Europe, and assassinating former Russian intelligence officer and defector Alexander Litvinenko by burying the highly toxic radioactive element polonium in his sushi in London in 2006.

★ ★ ★

Active measures are one manifestation of the asymmetric approach to competition that all U.S. adversaries are now using against us. Asymmetric attacks are about attacking in a roundabout way rather than directly confronting, using surprise and the unexpected, draining power through creating costs, and finding ways to turn weaknesses into strengths. They have traditionally been the tool of the insurgent and the terrorist. But now they are increasingly the tool of anyone trying to confront an immensely powerful United States.

Consider the images in the summer of 2023 of a U.S. F-22 fighter jet shooting down a Chinese hot-air balloon with an AIM 9X Sidewinder missile. The jet cost more than two hundred million dollars, the balloon just under half a million. It’s basically the equivalent of killing a mosquito with a cruise missile rather than a flyswatter—a perfect illustration of asymmetric competition. The United States fields complex and costly capabilities against much cheaper, riskier, and more creative approaches taken by our adversaries. Asymmetric threats are not just embarrassing and cumbersome, but they weaken U.S. national security and create a cost imbalance that compounds the problem.

Asymmetry can be powerful. We would do well to take heed that the Roman Empire did not fall because of the attacks from the Persian Empire

or Carthage, but through the asymmetric threats that eroded its power, originating with comparatively small barbarian tribes. Even the most dominant nations must be concerned about asymmetric attacks.

The job of intelligence is to predict, understand, and respond to the unanticipated, the unimaginable, the unthinkable. This is the mission of preventing strategic surprise. Ideally, it means overcoming the asymmetric advantages of smaller, weaker adversaries who repurpose cheap or old tech to trigger an outsize, expensive U.S. response.

But asymmetric threats are hard to confront for a reason: they fall between the cracks. The IRA was not the KGB or the GRU; it was a company. U.S. intelligence agencies don't have a mandate to deal with domestic elections issues; that is a job for law enforcement. And even for law enforcement, addressing these types of threats is dicey, because it can easily start to look like election interference, to the perceived benefit of one side or the other. Regardless of what people theorize, Facebook or other social media companies sharing data with the CIA on American citizens is extremely difficult and laden with bureaucratic, legal, social, and political hurdles. These are the cracks that asymmetric foes know how to exploit, and the need for completely different ways to address these threats is one of the main forces driving the fourth intelligence revolution.

★ ★ ★

Russia is not the only entity using asymmetric threats that accelerate the intelligence revolution. Iran and North Korea remain highly dangerous secondary concerns. Armed non-state groups like ISIS, Hezbollah, and Al-Qaeda are also still threats. Adversaries have always accelerated revolutions in intelligence, and these are the adversaries driving our intelligence revolution now.

Sometimes our animosity with an enemy is overt, direct, and complete. Such is the case with North Korea, a country that presents two extremely difficult challenges to U.S. intelligence. First, it is by far the most totalitarian state on earth, which makes it almost impossible to have Americans get anywhere near a North Korean person or place. Second, the North Koreans have been dedicated to obtaining nuclear weapons and

intercontinental ballistic missiles at any cost, including the creative use of highly asymmetric cyber and criminal activities.

It's hard to comprehend just how totalitarian North Korea is. Its borders are heavily protected by the fourth-largest army in the world—1.3 million full-time soldiers and 600,000 additional reservists, about 5 percent of the population. To put this into perspective, if the United States had 5 percent of its population in the military, we would have 16.5 million soldiers. (We have around 2 million active service members, which is less than 1 percent of our population.) It's extremely difficult for foreigners, especially Americans, to enter North Korea, and even harder for North Koreans to leave. The punishment for breaking the law in North Korea can be more extreme than anywhere else. For example, North Korea practices generational punishment. This means that if someone commits certain political crimes, not only will they be executed or sent to a concentration camp, but three subsequent generations of their family will also be forced into lifelong hard labor. As you can imagine, Cold War–style case officers aren't recruiting many spies at embassy dinners in Pyongyang. Instead, we must rely largely on satellite imagery and other standoff approaches to gather information about what is happening above the 38th parallel.

North Korea can keep everyone out, a great protective mechanism, but it still must have offensive capabilities. As with Russia, China, and Iran, North Korea has turned to the use of cyber operations in its asymmetric competition. Cybersecurity vulnerabilities are the chink in the armor of the world economy and, in particular, of U.S. society. Such attacks can be used to steal intellectual property or money, collect American citizens' data, implant sabotage mechanisms into critical infrastructure, or any number of other harmful threats. One aspect that North Korea excels at is criminal cyberattacks. When we think of someone breaking into bank databases and stealing money, we usually think of lone hackers or, perhaps, criminal gangs of them. But North Korea has industrialized this kind of criminal activity to obtain cash, especially U.S. dollars, to fund its nuclear ambitions or, as is also likely, the Kim family's luxurious way of life.

To fund its nuclear program, North Korea has reportedly stolen over three billion dollars in cryptocurrency since 2017, using phishing attacks,

malware, and other cyberattacks. In a phishing attack, the hacker sends an email or text message that appears to be from a legitimate source, like a cryptocurrency exchange. The email or text will typically contain a link that takes the victim to a fake website that looks like a legitimate one, where they will be prompted to enter log-on credentials, thereby allowing the hacker to access the victim's account to transfer cryptocurrency out of it. North Korean hackers also use malware, including ransomware and Trojan horses, to steal cryptocurrency. Ransomware involves encrypting a victim's computer's contents until they pay a ransom. A Trojan attack is when a piece of software appears to be legitimate but is malicious and attacks a computer. North Korean hackers also use more straightforward methods, like social engineering, which involves manipulating victims into giving up sensitive information, such as passwords or account numbers, by posing as customer support.

Again, as with the IRA, we see how cybersecurity-using adversaries slip between the cracks. In this instance, they do so by crossing the line between criminal activity against commercial companies and individuals (monitored by the FBI and law enforcement) and national security activity funding a nuclear program (monitored by intelligence agencies like the CIA), thereby making it hard for the Intelligence Community to keep up. It is not just North Korea. China, Russia, and Iran all have government and mercenary units assigned to hacking U.S. government, corporate, and personal computers. We are in the midst of a worldwide cybersecurity war, with thousands of hacks per day.

It's not only money North Korea is after. Sometimes it wants revenge. In retaliation for the release of the movie *The Interview*, a satire (starring Seth Rogen and James Franco) featuring an assassination scene involving North Korean leader Kim Jong-un, the country launched a 2014 cyberattack on Sony Pictures Entertainment. It gained access to the company's network by sending Sony employees malware-laden emails it then used to steal and leak confidential information, including internal emails, employee data, and unreleased films. The Koreans also launched "distributed denial-of-service" (DDoS) attacks, disrupting Sony's online operations and preventing access to its websites and servers; it also issued threatening messages demanding

that *The Interview* not be released. The attack caused large financial losses for Sony and sparked a debate about freedom of expression and the potential for cyberattacks to stifle artistic endeavors. What's especially novel and concerning about the attack is that it was specifically targeted at a corporation, not a government entity. Asymmetry can involve not only the tools of the attack but also the targets of attacks. Instead of going after the U.S. Army Second Infantry Division, they went after Seth Rogen.

★ ★ ★

Many Americans saw on their news feed in January 2020 that a man named Qasem Soleimani had been killed by a U.S. drone strike near Baghdad Airport. Most probably wondered who Soleimani was and why his death mattered. Those of us in the intelligence world knew exactly who he was. The silver-haired sixty-three-year-old was one of the most dangerous men in the world, personally responsible for the deaths of hundreds of Americans and thousands of others. For twenty years, Soleimani had led the Quds Force, the part of Iran's Islamic Revolutionary Guard Corps (IRGC) responsible for intelligence, covert action, and paramilitary operations. Unconventional warfare is its stock-in-trade: assassinations; state sponsorship of terrorism; and aiding proxy insurgencies in Iraq, Lebanon, Yemen, and elsewhere.

Iran's asymmetric superpower is using proxies; the Quds Force and Soleimani were experts at it. Iranian offshoots and trainees include Hezbollah, a Lebanese Shi'a militant group formed after the start of the Lebanese Civil War. The IRGC helped train and fund Hezbollah from very early on. Iran has also backed Hamas in Israel to further its own geopolitical aims. Another group that the IRGC has trained, supported, and provided weapons to is Ansar Allah, which some refer to as the Houthis, the name of the Yemeni tribe that makes up most of the organization.

Each of these groups has its own goals and motivations separate from Iran's, but Iran is able to leverage its support to influence and control them, to a degree. There is an innate tension in any proxy relationship. Imagine, for example, Charles de Gaulle and his Free French Forces. Yes, the British supported them, but to say that de Gaulle was simply an arm of Churchill

and Britain is false. Notoriously, de Gaulle had his own agenda and made it clear he was going to get what he wanted. The degree of control in a proxy relationship ebbs and flows over time, but at its core, it is a transactional situation. Iran provides funding and training, which Hezbollah can use to pursue its goals within Lebanon—say, to force out the Israeli army or gain power in Lebanese elections (both of which, by the way, are also good for Iran). In exchange, Iran can influence and, to some degree, control the group and use it to further its own geopolitical goals. These could include attacking Israel when Iran deems it strategically necessary, carrying out terrorist and military missions elsewhere, and extending Iran's intelligence-gathering capabilities into Israel and other places, such as West Africa, where Hezbollah maintains a presence by hiding in the Lebanese diaspora.

Proxies give Iran plausible deniability. As with Russia and the IRA, it can be dangerous for Iran to confront the United States directly. But by having, say, the Houthis launch rockets at Western shipping in the Red Sea, Iran can plausibly deny involvement and keep the United States from attacking it. Does U.S. intelligence know that it is Iran backing and directing the Houthis? Yes. Is this just theater, then? Yes. But, weirdly, that theater is good for both sides, as the United States may also not want to attack Iran directly, which would set off a much bigger war that may not be in our interest. This makes intelligence operations against Iran complicated, as not only is it necessary to infiltrate and spy on Iran, but now we must also infiltrate and spy on Hezbollah, Hamas, the Houthis, and other proxies.

Proxies are also a resource-efficient means of pursuing geopolitical aims. Think of Quds and the IRGC as investors. By putting a little money into Hezbollah or the Houthis, they can extend their reach into many other places. Hezbollah can provide all sorts of intelligence sourced in Lebanon as well as from the Lebanese diaspora around the world. It is expensive for intelligence agencies to operate globally. They may not speak the local language or have the right connections. Maintaining people at embassies and setting up cover businesses is also very expensive. Operating through someone else keeps your costs down. It's the same for covert operations or military action. An Iranian base in Yemen would be expensive, but by backing a motivated Houthi rebellion, Iranians get similar results, like the

ability to fight a proxy war against Saudi Arabia or exert pressure on Western shipping. Asymmetry is as much a cost strategy as a national security strategy. And Iran is not the only country to use it; many others have turned to proxies to support their geopolitical objectives.

Even our own government has used proxies for exactly the same reasons. After the 1979 invasion of Afghanistan by the Soviet military, the United States set up a decade-long proxy war against the Soviet Union. CIA covert action and paramilitary officers provided training, equipment, and strategic and tactical advice to multiple Afghan armed groups, the mujahideen, which were used to fight the Soviets. Some of this support, such as the supplying of Stinger surface-to-air missiles, helped to turn the war by allowing the Afghans to shoot down Soviet attack helicopters and other aircraft. Covertly backing the mujahideen gave the United States plausible deniability and was a cost-efficient option to indirectly harm the Soviet Union. But, remember, the use of proxies is a double-edged sword, as they also maintain their own goals and separate loyalties. One of the armed groups that the CIA did not directly back, but that no doubt gained resources, training, and expertise indirectly, was Al-Qaeda.

★ ★ ★

Terrorists are the ultimate asymmetric threat. Not being states themselves, they lack many of the tools that one state can use to challenge another and, therefore, must turn to almost pure asymmetry. Knowing that states are much more conventionally powerful, insurgents use guerrilla tactics, such as never attacking large forces but instead trying to pick off smaller ones or making hit-and-run-style attacks. Terrorism takes this strategy one step farther. The core concept of terrorism is to use public violence as a tool to achieve a political aim. These relatively small, highly dispersed groups act secretly to evade state intelligence and law enforcement. They don’t attack hardened targets like military bases. Rather, they go after soft, civilian targets, ranging from office buildings to buses, to create as much public fear as possible. Dispersed groupings and unconventional tactics make it particularly difficult for states to find, much less defend against, terrorist threats.

When executed to perfection, terrorist attacks can threaten even the most powerful nations, as Al-Qaeda did on 9/11. For two decades after 9/11, U.S. intelligence agencies did everything they could to counter the asymmetric approach of terrorist groups, and this was the driver of the third intelligence revolution. This shows just how powerful asymmetry can be.

Authoritarian adversaries drive revolutions. Total war with Nazi Germany and Imperial Japan drove the United States to its first intelligence revolution; the Soviets to its second. The third revolution in intelligence was driven by Al-Qaeda and other terrorist groups. The next intelligence revolution will be driven by what may be the biggest threat yet to the United States and our way of life.

OceanofPDF.com

5

Enemy Number One

In the summer of 2021, a group of People's Liberation Army officials gathered at a launchpad in China. The commander gave the order, and the missile blasted off. The menacing spear tip went into orbit and then came back into the atmosphere at hypersonic speed, five times the speed of sound. (Its exact speed is classified.) At that speed, the air molecules touching the surface of the missile create so much friction that missile temperatures can reach 4,000 degrees Fahrenheit. To put this into perspective, the melting point of titanium is 3,034 degrees.

The missile flew around the world—in total, traveling over 24,000 miles—before returning to China. Unlike ballistic missiles, which are fired into space, orbit the earth, and then come crashing down in an arc, this hypersonic missile could maneuver at low altitudes at extremely high speed. This makes it incredibly hard, some say near impossible, to shoot down. Moreover, what's particularly threatening about this type of weapon is that it could evade our radars by approaching from the south or could even, potentially, loiter indefinitely, by skipping on the atmosphere, and attack at a time of the enemy's choosing. After traveling around the world, the Chinese missile narrowly missed its target back in China.

If you ever wonder what keeps generals at the Pentagon up at night, now you know: it's this missile. As the most senior person in the U.S. military at that time, Chairman of the Joint Chiefs Mark Milley, said, "I don't know if it's quite a Sputnik moment, but I think it's very close to that. It has all of our attention."

Hypersonic missiles may be the most dangerous weapons ever created. They are extremely difficult to track and intercept, and they can carry nuclear warheads. This means that the Chinese military could launch a strike on any country without warning or recourse. The message came through loud and clear: China is a major military power, capable of projecting that power anywhere in the world—even into the heart of the continental United States.

Hypersonics are part of China's anti-access/area denial (A2AD) military strategy, the ultimate asymmetric military competitive approach. The Chinese People's Liberation Army, or PLA, knows that it cannot compete militarily with the United States directly for the time being. We just have too many aircraft carriers, missiles, fighter jets, and, most important, too much combat experience. Knowing this, the PLA focuses its resources on limiting our ability to create threats close to the Chinese homeland. This means a strategy of using missiles and other weapons that are relatively low-cost but that can ward off anyone who tries to come close. This could look like using thousands of missiles to shoot down any incoming U.S. aircraft; or an ICBM to blow up an aircraft carrier in the western Pacific; or swarms of small boats, even fishing vessels, that can ward off any U.S. Marine Corps amphibious force. Meanwhile, the PLA is also building up a large nuclear force, which acts as a strategic deterrent, just as the Soviets did during the Cold War.

The competition over hypersonic weapons is just one aspect of the wider battle for power and influence. There is a much broader competition over worldwide dominance between the United States and China, the world's two largest economies and two most powerful militaries. While arguably China may be ahead right now in hypersonics, the United States is ahead in many other areas, from AI to biotech to traditional military superiority. Nonetheless, the fear is that China has such a large economy and industrial capacity, with fewer limits on how its government can maneuver, that it can catch up and surpass the United States in many, if not most, of these areas. It's a more complex and multifaceted version of the Cold War, playing out in a number of areas, including markets, technology, and military might. This strategic competition between the United States

and China is pushing, and will continue to push, the accelerator on the already rapid transformation in how we conduct intelligence.

★ ★ ★

The competition appeared to come out of nowhere, but that was planned and purposeful. Deng Xiaoping, who served as China's paramount leader from 1978 to 1989, notably summed up the Chinese attitude as "Hide our strength, bide our time." This mantra effectively described China's approach for decades. The Chinese pretended to be friends and partners with the United States, an extension of the rapprochement after Henry Kissinger and Richard Nixon's visit to China in the 1970s, and integrated into the global economy. Over time, China built up its economic and military might, becoming the world's second-largest economy, a key supply chain provider to almost every aspect of the U.S. economy. It also invested strategically in complex military programs, including hypersonics. This was a decades-long plan. That time is over; China no longer hides its strength.

Xi Jinping, China's paramount leader since 2012, has built the Chinese economy into a juggernaut, has dramatically increased military and intelligence capability, and has not been afraid to flex his nation's powerful new muscles. This new assertiveness in diplomacy is colloquially referred to as wolf warrior diplomacy, after a jingoistic Chinese action movie akin to *Rambo*. Xi explicitly and publicly calls for China to lead the world economically and militarily by 2049, the one hundredth anniversary of the communist revolution in China. He has developed multiple signature power programs like the Belt and Road Initiative and Made in China 2025, used economic power as a means of geostrategic bargaining, cracked down on dissent in Hong Kong, and become extremely aggressive about annexing Taiwan. He also represses political opposition internally in a way that is far more sophisticated and totalitarian than any nation in history could ever have dreamed.

China combines the military and autocratic focus of the Soviet Union with a very strong economy—a powerful and concerning combination. In the past, our biggest competitor, the Soviet Union, could never compete with us technologically except in narrow areas such as missiles or nuclear

weapons. China is rapidly catching up in almost all technological areas and surpasses us in some. The Soviets also always had a much smaller economy than the United States, but China will soon have an economy larger than our own. A bigger economy means a bigger tax base, which means the capacity for a larger military budget. When it comes right down to it, a military's power is very much determined by how much you can spend on it. It is a terrifying prospect that China could one day have twice the military budget of the United States and, from there, potentially an overwhelming military advantage.

Yet, although China is our biggest threat, we remain relatively friendly with the Chinese. As you read this, you are likely wearing something made at least in part in China. You could easily hop on a plane to Beijing tomorrow. A restaurant in Shanghai is serving tofu made with U.S. soybeans at this very moment. This is hardly the dark days of the Cold War.

The major reason we have not devolved into Cold War–esque engagement with China is that, unlike with the Soviet Union, we have an economic interdependence with China that is extremely hard to break. This became very evident during early days of the Covid-19 pandemic, when it was difficult to obtain masks, hospital gowns, and other personal protective equipment. China produced nearly all that equipment but had stopped exporting it to the United States. These were simple fabric and paper items, yet we could not produce them at home in the quantities and at the speed we needed. That is just the tip of the iceberg. There are thousands of important items we cannot produce in the United States, from medications to tractors. If we were to sever ties with Beijing tomorrow, the U.S. economy would fall apart and people would suffer, as we would run out of everything, from minerals to essential medicines to batteries.

Thankfully, this dynamic is not one-sided. China is in a similar bind. It requires many goods from us, such as semiconductors and food. And because the Chinese economy is much more focused on exports than ours, China needs the United States as a trading partner. While rebuilding a U.S. supply chain without dependence on China would take years and require great costs for some very important items, like rare earth minerals and pharmaceuticals, the same is true for China. For now, our dance with China

feels like two fighters, each with a knife in one hand and the other hand tied to that of his opponent. The two adversaries circle each other, unable or unwilling to fully strike and yet also unable to turn around and walk away.

Given this bind, China and the United States must turn to forms of competition other than all-out war. This still includes military facets. Both the United States and China are developing new military technologies for deterrence, from hypersonic missiles to spacecraft to autonomous drones. Both militaries perform a delicate choreography of military threats in the South China Sea and elsewhere. But most of our competition is nonmilitary in nature. Cyber warfare is used to infiltrate and disrupt networks. Both nations compete diplomatically for influence in key regions, such as Southeast Asia, Africa, and the Middle East. Economically, we compete over everything from critical minerals to semiconductors to talented AI engineers and biotech scientists.

Intelligence is one of the most important areas of this competition because it underlies many of the other areas of competition and because it can be done out of sight. As during the Cold War, this intelligence competition keeps us both prepared for war and, we hope, out of war. Toward this intelligence competition, China has built the typical intelligence capabilities.

Like all nations, China uses intelligence to protect itself militarily and to support its political and diplomatic decision making. The Ministry of State Security (MSS) is China's central intelligence agency, but with powers, authorities, and responsibilities that are much broader than those of the United States' CIA. In essence, the MSS operates an intelligence agency, a secret police, and a security agency simultaneously, similar to the KGB. The MSS is joined by the Chinese military intelligence service, the Intelligence Bureau of the Joint Staff Department of the Central Military Commission, which functions in a manner somewhat similar to the United States' DIA or the Russian GRU.

These agencies perform all the usual forms of intelligence necessary to maintain national security. They recruit human intelligence sources with placement and access to national secrets—like the CIA. They launch and operate satellites that use sensors to spy from above—like the NGA and the

NRO. They perform signals intelligence to collect radio, cell phone, electronic, and other forms of signals and communication—like the NSA. They use cyber operations to collect information from secure computer networks, whether classified or not. This is the normal meat and potatoes of intelligence agencies.

While the Chinese intelligence organizations have similar missions and somewhat similar organizational structures, they differ greatly in their approach to intelligence. China is building what may be the greatest and most totalitarian intelligence and security system ever devised. This system not only controls its people but is extended to threaten all of us.

★ ★ ★

To fully understand Chinese intelligence, we need to return to the ’80s, the *17*80s. During that time, the English philosopher Jeremy Bentham invented a concept of diabolical genius, the panopticon. It was a plan for a type of prison in which a single guard could stand watch in a central guard tower. The prison cells were then laid out around that tower so the guard could see into any cell without needing to move from his location. The inmates could not see into the tower, so they could not know when or whether they were being observed. The idea was that inmates would assume they were being observed at all times, and thus were implicitly threatened by violence at all times for transgressions, so they would regulate their own actions. Bentham was a social reformer who truly wanted to help make prisons better. He did not imagine—indeed, *could not* have imagined—that this all-seeing concept could leak out of prisons and into an entire population.

The CCP is attempting to create a global panopticon. Rather than Bentham’s guard standing in the center of the prison, a global panopticon relies on data collection rather than eyesight. By collecting and analyzing all the data in the world in real time, Chinese intelligence could sense everything that was happening and, potentially, even predict what people might do. From there, it would be able to implement a system of social control through censorship and threat. Not only are the Chinese trying to build such a system, but they’ve already essentially succeeded within China.

The first step in this process of constructing a global surveillance panopticon is collecting all the intelligence. China uses the tried-and-true method of intelligence sources to collect data. It's been estimated that sixteen million people, or a little over 1 percent of the population of China, are political informants to the government. That is a similar number to the East German Stasi's, or secret police's, recruitment during the height of the Cold War. These sources have been put to use, with an estimated thirteen million people under surveillance, equivalent to more than the population of Belgium. But China goes much further than old-fashioned informants.

The Chinese secret services have turned to the mass collection of data to surveil the nation's billion-and-a-half people. In 2021, China enacted its Personal Information Protection Law of the People's Republic of China, which in theory provides protections for its citizens' data. While this law might read like privacy laws in the United States or the European Union, in practice, there are no real privacy protections that prevent the Chinese government from collecting data. In fact, all Chinese companies and, indeed, all Chinese people must provide any requested data or information to the government upon request. China's 2017 National Intelligence Law states that "any organization or citizen shall support, assist and cooperate with the state intelligence work." In practice, a Chinese company or person is legally required to provide Chinese intelligence agencies with any information about anything, including about themselves. This is the nature of the authoritarian government in China, where all personal rights are subservient to the needs of the party and its leadership.

Beyond the National Intelligence Law, every major company must have a CCP cell within it. These cells, made up of Chinese Communist Party members, act as a means of communication, indoctrination, and control between the company and the CCP. Every public company in China has been required to have such a cell since 2018, and most other relevant companies also have one. In 2020, China began requiring that all state-owned enterprises have a cell. The Securities Regulatory Commission in China has also gone so far as to order that there be party cells inside foreign financial firms. The CCP members inside the companies can collect information and data, influence company decisions, appoint people to

boards, and at times control company functions. Such mechanisms are the means through which the CCP can formally and informally direct companies to carry out the party's wishes.

More generally, the CCP can punish CEOs and other business leaders who do not comply with their requests. Even the most powerful CEOs are not immune. The founder and former CEO of Alibaba, Jack Ma, is one of the richest and most powerful business leaders in China, if not the world. Yet, in 2020, he disappeared from the public after apparently running afoul of the CCP after he criticized regulators. He later reappeared in Japan, where he was teaching, and only in 2024 did he again make a public comment on Alibaba. Other CEOs have similarly disappeared from the public. While China can sometimes seem like a modern capitalist economy, it is still underpinned by an authoritarian dictatorship that can and does use force to get what it wants.

This sort of control means that any Chinese citizen can be required to act as an agent and, thereby, can be a potential national security threat. Now, of course, there is more subtlety to it than that. Not every Chinese citizen has access to information of any value, and even among those who do, not everyone would be asked for it by their intelligence service, which, like any other intelligence service, has bandwidth limits. It is not as unusual as it sounds for citizens to be asked to provide information to their national intelligence service when needed. Half of all spy movies begin with a regular person being approached by a CIA or MI6 agent and asked to provide information on their recent trip to the Soviet Union or something along those lines. It is not common, but it's accepted in the West as well. The difference is that all Chinese citizens are *required* to do so, and there is no legal recourse should they wish to refuse. This is not the fault of the Chinese people; in most cases, they are explicitly or implicitly forced to act on the behalf of the CCP, whether or not they are a CCP member. It is the harsh reality of living in an authoritarian nation.

What is most concerning about this system is that all Chinese companies must provide their data to Chinese intelligence. Every Huawei router must be accessible to Chinese intelligence. Every video filmed on TikTok, every financial transaction that involves a Chinese bank, every DJI

drone feed, every battery management system diagnostic data feed on any device, and every genetic sequence performed by a Chinese biotech company or on Chinese equipment—all must be accessible to Chinese intelligence. Chinese intelligence services have created a state in which all forms of data collection and sensors are or can be fed into government databases.

The Chinese approach to intelligence is to vacuum up everything they can. It is an entirely different strategy than that of the United States, which is focused on reconnaissance or collecting data as needed. It is the epitome of totalitarian surveillance.

The doors to all data are open to Chinese intelligence, and there is now more data than ever to collect. China is experiencing a massive, society-wide proliferation of digital technology—propagating data collection across every aspect of life. Just as in the United States, Chinese citizens are increasingly spending their lives on cell phones and other digital devices, in which all activity is tracked and can be monitored. New technologies—from 5G to genetic sequencing to generative AI chats to autonomous cars—are connecting more devices to the internet or collecting more types of data than ever, and all of it is being fed into the panopticon system.

The next step after collecting all this data is to monitor it. For decades, surveillance has been limited by how many people can monitor the surveillance devices. The panopticon solves this problem because even if everything is not in fact being monitored at all times, the imagined *threat* of its being monitored still creates control. However, soon enough, with the power of AI, the limit of human monitors will be ended, as AI systems can actively monitor everything at once.

The ultimate use of this data is for control, and the Chinese surveillance state has led to a whole new form of social control called the social credit system. The collected data points—travel records, reading and social media habits, purchases, texts exchanged with friends and associates, everything—are woven together by algorithms to provide a “social credit score.” It is somewhat similar to a credit score you might use to take out a car loan, except it includes everything about a person, not just financial information, from their political loyalty to their personal relationships to

their criminal record. Think of it as a file on every man, woman, and child in China that contains all the relevant data on that person, updated constantly and accessible to Chinese security services.

This score is then used for control, by providing Chinese citizens with privileges or removing those privileges. For example, those with a low social credit score may not be able to take airline flights or attend certain schools. The scores are integrated with surveillance systems in public places, meaning that anyone entering a public space and identified by facial recognition software could have their social credit score used against them, or their actions in those spaces could be added to their score. Such surveillance and scoring are becoming an everyday part of life in China that feels like an episode of *Black Mirror*.

The social credit system is based on the mass data collection and recommendation systems used by technology companies. Tech behemoths like Google and Facebook track all the activities of their users and then employ complex algorithms to derive insights into users' behavior, using those insights for action. In the case of U.S. companies, these insights are generally used for targeting advertisements. There are rules around data collection in the United States, and the data collection is highly compartmentalized. Google has no access to IRS tax records or criminal records, for example, and the IRS has no access to Google's data. China has taken a radical approach, collecting and employing much more comprehensive data about people than any U.S. company or government agency could ever imagine.

Society-wide surveillance in China and the country's social credit system are about control. Sometimes it is literal and immediate control. Within minutes of its being posted, a story or even a word can be censored in near real time. More generally, the control is about the threat that anything you do will be seen and could lead to punishment. When ethnic Uighurs are faced with the very real possibility that being seen reading the Quran might put them in a concentration camp, most will opt not to read it, certainly not in any group or place that could be monitored. A true panopticon like this does not even require secret police to do much to

enforce control; people will enforce it upon themselves. This is what a society-level panopticon looks like.

China is heading toward a reality in which the lives of its 1.4 billion citizens will be monitored at all times and thereby controlled; indeed, in some ways, that reality is already here. This is a project to perfect totalitarianism.

The terrifying thing is that China is not stopping at its borders. It is actively attempting to export this panopticon to the rest of the world, especially the United States. If it is already monitoring 1.4 billion people, moving on to monitor the other 6 billion in the world is fairly straightforward. Certainly, adding 330 million Americans is trivial.

While Chinese internal data collection nears perfect monitoring, the Chinese intelligence services are also collecting as much foreign intelligence as they can, including on Americans. There are innumerable reports of Chinese devices sending user data back to China. Though it denies it, TikTok has been found to send its users' social media data, including that of children, back to China. And despite repeated denials by the founder and CEO of Huawei Technologies, Ren Zhengfei, it is clear that Huawei has the ability to obtain data from U.S. or other networks that use its systems. And where Chinese companies cannot get the data, China turns to more illicit means.

The next time you see a story about a dataset being stolen or Chinese hackers breaking into a database, know that they are collecting all your data to build up the same database China has for its own citizens. In 2015, China stole the records of every American with a security clearance from the U.S. Office of Personnel Management. It has stolen credit, health care, genetic, and many, many other datasets. As a 2021 report from the National Counterintelligence and Security Center (NCSC) dryly noted, "Through its cyber intrusions in recent years, the PRC has already obtained the Personal Identifying Information (PII) of much of the U.S. population. Recent breaches attributed to the PRC government or to cyber actors based in China include … the theft from Marriott hotels of roughly 400 million records; the theft of data from Equifax on roughly 145 million people; and the theft of data from Anthem on roughly 78 million people."

Yet Chinese intelligence has gone much farther than just stealing data; it is also hacking into U.S. systems to obtain real-time intelligence on us. In 2024, a Chinese hacking group referred to as Salt Typhoon penetrated the phone systems of AT&T, Verizon, and other companies and gained direct access to Americans' calls and text messages. The hackers had broken into the system that U.S. law enforcement uses to legally access calls as part of its investigations. It was another example of parasitic asymmetry—there is no need to hack into every phone company when you can just use your adversaries' technological systems against them. This hack also shows how the systems built up during the last intelligence revolution, especially centralized surveillance, are now a vulnerability that needs to be rectified in the next revolution, ultimately by again decentralizing surveillance.

Salt Typhoon also shows just how powerful a tool offensive cyber hacking can be for espionage. Such hacks can have massive ramifications for national security. In this case, it appears that Salt Typhoon specifically targeted the phones of Donald Trump and JD Vance as well as other government officials. Moreover, they have been able to access nearly anyone's private texts and could even record phone calls, making the entire American population a potential target. This Chinese hacking is a taste of where China hopes to go, extending its surveillance network beyond its borders to America and the rest of the world.

Unfortunately, Chinese intelligence doesn't even have to steal much of this data; for years, they have been able to simply buy it on the open market. Chinese companies have taken advantage of the fact that the United States has few safeguards on selling commercial data. Everything—from mobile movement data that tracks where your cell phone and, therefore, you move, to your browsing history, to your financial records—is available for purchase on the open market. In fact, even your most personal health data is available. As one NCSC report stated, "China's BGI [a genetic testing and analytics company] purchased U.S. genomic sequencing firm Complete Genomics in 2013." The report also notes that "Chinese companies have also gained access to U.S. healthcare data by partnering with hospitals, universities, and other research organizations in America." Remember, anytime a Chinese company obtains access to your data, it must provide

that data to Chinese intelligence. Hence, when you read a sentence like "Chinese companies are partnering with American hospitals," you can be sure that whatever data they get access to at that hospital is going right back to a CCP database.

The United States has tried legal means to prevent China, Russia, and other adversaries from being able to buy Americans' data. Cognizant of the threat, in 2024, the Biden administration enacted an Executive Order that limits countries of concern, including China, from accessing Americans' data through various rules and policies. Yet this is likely too little, too late. China can continue to find ways to obtain U.S. data, whether that means stealing it with cyberattacks, recruiting sources to access it, or maintaining backdoor access through internet-connected Chinese electronics that are used by pretty much every American every day.

The ultimate goal for the Chinese Communist Party and its intelligence services appears to be the same for Americans as for the Chinese people—to create a system of social control. All that financial, health care, movement, social media, and other data can be added to a database and then used to create a dossier on a person. This dossier can be used to rate that person in any way China wants. In essence, it is like the Chinese social credit score. Maybe it's loyalty to the government or a company, which is useful when trying to recruit an asset; or susceptibility to disinformation campaigns; or openness to being bribed. As the data gets closer and closer to real time, it can be used to track people, literally tracking their mobile phones as they move around or their browsers as they skim articles on the internet. This monitoring system can thus be used to surveil someone for their entire life and tailor disinformation to them. If you have ever wondered why you keep seeing massive database hacks of your medical records or financial information, this is why, and hopefully it illustrates why you should be concerned.

The Chinese approach to societal surveillance is the ultimate asymmetric form of competition. Instead of needing to find a way into the toughest spots—that is, classified systems and military bases—it targets our soft underbelly by collecting all the relatively unprotected, seemingly unimportant information in our society. That doesn't mean China ignores

traditional military or other issues. The mobile movement data bought by a Chinese innocent-seeming intermediary, or cut-out, firm could also contain the movements of an American general or congressman. The medical information China obtains through a hospital partnership could be that of a CIA officer or their spouse. Or a hacker group could hack into the database of a major supplier of parts to a defense contractor building fighter jets. The point is that this information is much easier to collect, there is much more of it, and it is incredibly important in today's most competitive areas, from the economy to science and technology.

China is going farther than just this surveillance form of asymmetric competition to a far more expanded view of what intelligence should do. Conceptually, the reason China is so powerful as an adversary, beyond its size and military capabilities, is that it has instituted a true whole-of-society approach to competition. This includes not only the traditional forms of state power, like diplomacy and the military, but also economic competition, competition over technology, and several other areas. For some time, this has been referred to as unrestricted warfare, which was the title of a 1999 book by two colonels in the People's Liberation Army that touts an approach targeting an opponent's entire society—including its economy, political and legal systems, morale, and public opinion—alongside its military. Such unrestricted warfare is the ultimate form of asymmetric competition because it slips around the core strengths of the United States and hits us where we have no defenses.

Meanwhile, China has also focused on the flip side of the asymmetry by making it extremely difficult for the United States to collect intelligence about China. Information about everything from politics to the economy in China is regularly censored. Little government information makes it online, as it does in the United States. U.S. consulting and related companies inside China have been legally limited in what they can research or even shut down, making economic and commercial data collection difficult. There are simply fewer Americans in China and learning about China. In 2024, around seven hundred Americans were studying abroad in China, while around three hundred thousand Chinese were studying inside the United States. There is very strong counterintelligence protecting China's

government and also its people. The government has long warned the Chinese population that foreigners could spy on them. At one point in 2024, it explicitly warned Chinese students that “handsome men and beautiful women” could try to get them to give up secrets. The head of the MSS, Chen Yixin, announced that China’s citizens should “build a people’s line of defense for national security.”

Finally, China may have the most powerful of all weapons—sheer size. As in the quote often attributed to Stalin, “quantity has a quality all its own,” and China has the ultimate quantity. The nation’s population stands at around 1.4 billion. Its secret services are said to employ 600,000 people. The FBI has said that its cyber personnel are outnumbered 50 to 1 by Chinese cyber actors. Britain’s MI5 has said that more than 20,000 people in Great Britain have been approached by Chinese intelligence collectors since 2022. Assumedly, that number is as high as or higher than that for the United States. These are overwhelming numbers that are almost impossible to comprehensively defend against. And it shows. There are near-continuous online data hacks, IP thefts, drone spying, information attacks, and other intelligence operations targeted at the United States and our allies.

Today, we face another gathering storm. Decades ago, we faced such a storm with the rise and militarization of Germany and Japan. The United States was unprepared for that storm. Through sheer force of will, we raised the largest army in our history, turned our economy to produce weapons of war, birthed our first intelligence agency, and marched toward victory. Today, we too are unprepared. This time, we may be ready militarily to fight anytime, anywhere, and win. But our enemies know this, and so have turned to asymmetry to fight, and we are not prepared to compete. We must learn to fight in many different realms, many of which have nothing to do with the military or politics. One of the most important of those realms is intelligence. This time, the preparation looks far different. Unless we again steel ourselves for battle, we will succumb to this new rising storm of war. It is to confront this storm that we turn to the fourth intelligence revolution. The first facet of this revolution is the radical expansion of intelligence into new fields, beginning with economic espionage.

OceanofPDF.com

6

Embracing Economic Espionage

The impenetrable vault is hidden deep within CIA headquarters. And if the lead covert operations officer and his team are going to steal Top Secret files, they will have to get inside it. Disguised as firemen, the agents manage to sneak into headquarters and poison the vault guard. After handily diverting the laser beam that will search them out and set alarm bells ringing, the leader dangles headfirst into the vault, retrieves the equipment, and begins the download. In a tense moment, he almost drops to the floor when his partner holding the rope slips. A single drop of sweat hangs off his glasses, threatening to hit the motion sensors on the floor. At the last second, the officer manages to wipe it away, averting disaster. With a CIA officer about to enter the room and blow the operation, the covert operations officer's partner quickly hoists him back through the vent. Just as he is almost clear, a knife falls from his pocket, and the arriving worker, alerted to the intruder's presence, sets off the alarm.

This is of course a scene from the movie *Mission Impossible*, starring Tom Cruise as superspy Ethan Hunt. It is pretty much what we imagine when we think of espionage. Yet the reality, as is usually the case, looks a lot less exciting.

Here is more what espionage looks like in real life in today's world.

Zhang Hao seemed to be just another smart immigrant doctoral student enjoying life in Southern California after making his way from Hunan Province to the University of Southern California to study for a degree in electrical engineering. After getting his PhD in 2006, Zhang secured a coveted position as an FBAR (film bulk acoustic resonator) engineer at

Skyworks Solutions, a leading semiconductor company. FBARs are microelectronic components that have key uses in telecommunications equipment like cell phones. For the next four years, Zhang probably seemed like any other technology employee. As a part of his work, he had direct access to Skyworks's highly confidential technology related to critical components used in radio frequency filters and crucial to cell phone technology.

Zhang eventually moved back to China and became a professor at Tianjin University. He also co-founded a company called Novana, which focused on—no surprise—developing FBAR technology. These FBARs were sold both commercially and to Chinese military customers.

Little did Zhang know, the U.S. Department of Justice was on to him. After years of investigation, he was arrested when he flew to Los Angeles in 2015 to attend an academic conference. He faced charges of economic espionage and theft of trade secrets, and in 2020 he was convicted and sentenced to eighteen months in prison.

To translate this story: Zhang stole a strategic U.S. technology and brought it to the Chinese military. It doesn't sound much like Ethan Hunt stealing those secrets from CIA headquarters. Trade secrets were stolen from a company that made a product most of us had probably never heard of for an application we had never considered. There was no mention of a spy agency anywhere in the story, but what Zhang did was the equivalent of spying. In fact, it was no different from the Chinese MSS sending an operative to break into a vault and bring back technology to their military—except that this was much, much easier and less risky to do. This episode is, in fact, a textbook case of Chinese economic espionage tactics. While it may sound banal, by following this playbook, acts of economic espionage could have as much damage as an enemy breaking into our most secret intelligence agency SCIF.

An amusing anecdote I recall first hearing early on in my intelligence career gives a sort of shorthand for how economic espionage works with our various rivals. As one China expert summarized it:

> If a beach was an espionage target, the Russians would send in a sub, frogmen would steal ashore in the dark of night and with great secrecy collect several buckets of sand and take them back to Moscow. The Americans would target the beach with satellites and produce reams of data. The Chinese would send in a thousand tourists, each assigned to collect a single grain of sand. When they returned, they would be asked to shake out their towels. And they would end up knowing more about the sand than anyone else.

The anecdote may sound a bit flippant, and it's not entirely accurate, but it does illustrate some salient points. In a world in which China cannot yet compete militarily or diplomatically with the United States, it must find other, asymmetric ways to succeed. With a massive population that still relies on relatively low wages per capita, China developed a thriving economy once it went global two decades ago. This has allowed it to corner the market on many key ingredients in the Western supply chain, making the United States and much of the rest of the world highly dependent on Chinese trade. The United States no longer manufactured this equipment; China did, and we became dependent. That dependency gives China an entry point not only for economic growth but also for espionage. While China doesn't necessarily send tourists to beaches, it definitely sends employees like Zhang to important tech companies.

Economic espionage works well for the CCP also because economic secrets are poorly defended, compared to traditional national security secrets. Skyworks Solutions was a great soft target, as are so many other U.S. companies that can't adequately protect their data or their systems. FBI teams typically don't get involved in corporate business unless there are allegations of wrongdoing. Also, anyone with the appropriate technological training could go work for Skyworks Solutions, no clearance required. The technology itself was not built with anti-tampering mechanisms to prevent reengineering by adversarial companies. The points of entry for theft are seemingly endless. Skyworks Solutions is not unusual; most U.S. companies have the same weaknesses. It's not the company's fault; it is the

victim here. China has in many ways systematically set up its economy with the intent and purpose of enabling IP theft for strategic purposes.

Now imagine that beach full of sand as an economy with strategically important intellectual property. And instead of tourists on a beach, there are hundreds of thousands of people at thousands of companies, in hundreds of industries, all relentlessly taking grains of sand over decades. That is exactly what has happened. There is no need to mount a risky commando operation or expensive technical operation. Unfortunately, the Chinese approach to economic competition does not stop at shaking out sand—that is, it does not rely only on its massive population to pick away at soft targets bit by bit.

In the last several years, China has begun taking big swings in what is best characterized as economic colonialism. Hambantota Port in Sri Lanka is the perfect example of how China uses its capital toward strategic ends. As part of the Belt and Road Initiative, a Chinese program designed to invest in infrastructure across Asia, Africa, and Europe, the port project was set up with China by Sri Lanka's president at the time, Mahinda Rajapaksa. Despite feasibility reports that indicated the port would fail and run up Sri Lanka's debt, the loan went through anyway. After years of construction by one of China's state-owned enterprises (i.e., a company controlled by the Chinese Communist Party), the China Harbour Engineering Company, Hambantota Port was completed.

Just as the studies predicted, the port failed to garner attention, didn't make money, and defaulted on the debt. Sri Lanka wound up giving up the port and the surrounding 15,000 acres of land to China for ninety-nine years as collateral for defaulting on the loan terms. In the future, Hambantota Port could easily be transformed into a naval port for the Chinese navy, especially considering its prime location off the coast of India (a country China considers a strategic adversary, with which it has had deadly border clashes over decades, including one in 2020 that left dozens of soldiers dead). In essence, China used the machinations of a government-directed corporate debt deal to take over the sovereign territory of another nation for strategic purposes.

The consequences of economic competition and economic espionage are a big deal, but not always for the reasons you might assume. Yes, companies can lose market share to competitors who steal their technology, they can be forced to spend more money on security, or they can even go out of business. Those things are bad, but they are relatively minor nicks on the hide of the U.S. economy and have relatively little effect on national security. What does have a major effect is when China controls strategic industries, a powerful bargaining chip that can allow it to hold countries at ransom. For example, China mines 60 percent of the world's rare earths, processes over 80 percent of them, and manufactures over 90 percent of the rare earth permanent magnets in the world. These magnets are key components in iPhones but also in missiles and other weapons.

China is well aware of how to use such leverage to its advantage. In 2010, during a diplomatic disagreement over a ship collision, it cut off rare earth exports to Japan, creating an economic crisis. The United States' being cut off from rare earths today could create an economic depression, as many goods could not be produced, driving up costs to extremes. Worse still, it would undermine our ability to make weapons to defend our interests. It's an implicit threat. Even without actually cutting off exports, China can use its control for trade and other diplomatic bargaining.

The stakes for economic espionage continue to increase, even to the point of real-world violence. One example occurred in 2024, in what appeared to be attack by Israel on Hezbollah. Israel was able to get into the supply chain of pagers that Hezbollah had ordered for its troops. From there, it inserted explosive materials and likely some form of cyber vulnerability or electronic device into the pagers. Then, on September 17, 2024, it triggered thousands of these pagers simultaneously, killing some members of Hezbollah and wounding many others. This illustrates just how dangerous a supply chain vulnerability can be. Now imagine that instead of exploding pagers, the exploited supply chain vulnerability involved making U.S. F-22 fighter jets inoperable or shutting down American ports by knocking out every Chinese-made crane when the United States was in a war or other emergency.

★ ★ ★

As with any other form of competition, when China uses economic intelligence, it necessitates that the United States respond with its own. This is the rhythm of intelligence competition, as one actor moves from symmetric to asymmetric competition. The problem is that the United States has long minimized, if not completely ignored, this form of intelligence.

Some of the best economic intelligence I have seen did not come out of a classified briefing room or even from within the Washington, DC, Beltway; it originated from a quaint town on the Connecticut coast. After leaving the NGA, I moved on to join the hedge fund Bridgewater Associates. Founded by legendary investor Ray Dalio, Bridgewater invests hundreds of billions of dollars a year. More relevantly, it understands the global economic system better than any intelligence agency. Yet it employs only around 1,300 people. To put this into perspective, the U.S. Army Intelligence and Security Command (INSCOM) alone has 17,500 intelligence officers.

At hedge funds like Bridgewater, economic intelligence happens every day. Teams of researchers gather the highest-level analysis on micro- and macroeconomic news. They use commercial data and analytical tools such as a Bloomberg Terminal, which provides access to thousands of different financial and economic data points. Often, these researchers will turn to advisers with deep expertise in particular areas—like someone who spent thirty years working in the automotive industry or a PhD in economics who has studied the bureaucratic structure of Spain's central bank. They also use more esoteric alternative data, often called alt data, such as commercial satellite imagery or mobile phone movement data or algorithms that can help assess whether a company's CEO was exaggerating during an earnings call. This information is then analyzed to attempt to model out what is happening at every level, from the global economy to a nation's central bank to an obscure company. The final products are assessments of the current and future value of assets. The analyzed information can then be fed into trades in public equities, bonds, or commodities markets or used to

privately acquire a company. The driver for all this work is simple, trading markets are highly competitive, and only the best can make money.

Economic intelligence is not new to the United States. One of the first recorded instances of U.S. economic intelligence gathering was in 1776. The American colonies had declared their independence from the British Crown. The new United States of America had to be able to fund the war. Accordingly, the Continental Congress's Committee of Secret Correspondence—sometimes regarded as the first U.S. intelligence agency—sent American statesman William Carmichael, disguised as a merchant, to report on potential European competition in the tobacco market.

Economic intelligence continued to be an issue for U.S. intelligence over our history, but it was never a tier-one priority. During World War II, the OSS used economists to analyze the capabilities and intentions of enemies and allies. Throughout the Cold War, the CIA tracked the economic and production capabilities of the Soviet Union, so that by 1990, the former Director of Central Intelligence Stansfield Turner could claim, "We know more about Soviet grain production than they do." And while economic intelligence rose in importance and estimation during the Clinton, George W. Bush, and Obama administrations as the world became more globalized, it was not until the issue of President Trump's National Security Strategy that economic competition with China—and, therefore, economic intelligence—became a front-burner issue. President Biden's strategic competition doctrine heightened the focus and cemented it. However, the IC still lags considerably in its ability to perform economic intelligence at anywhere near the level needed in today's world.

In an echo of Stimson, U.S. intelligence agencies are under the impression that "gentlemen do not read each other's spreadsheets." This separation of the state and the economy is, like the separation of church and state, considered one of the foundations of American democracy. This has led to two major issues for economic intelligence.

One is that U.S. agencies cannot adequately collect and analyze economic intelligence. To understand the global economy, you must first understand the U.S. economy and U.S. companies. However, because the IC is loath to collect and analyze information about U.S. companies, and is

legally limited in doing so, it cannot really understand the issues in a comprehensive way. Second, even if U.S. agencies could adequately understand the economic and commercial issues, they wouldn't necessarily share this information with the companies that would benefit. This is because they might be accused of picking winners, one of the cardinal sins you can commit in the U.S. government.

These are fair concerns, but the issue is less black and white than we might have been led to believe. Intelligence and intervention have always been part and parcel of the U.S. economy. The firewall is an illusion, a narrative developed in recent history around globalization. The reality is that the U.S. government has intervened in the economy throughout its history, from rationing and control of defense production in World War II, to the use of Opportunity Zone tax credits for real estate investments in underprivileged areas, to the use of sanctions and export restrictions on adversarial nations. More to the point, the United States has taken part in economic espionage since the Revolutionary War, for better or worse.

That's not to say that we should have unadulterated government interventions for economic reasons, nor that the United States has always done economic espionage for good reasons. Take, for instance, the mid-century CIA's plan to intervene in a Guatemalan election. When Guatemala's democratically elected president Jacobo Árbenz passed an Agrarian Reform Law in 1952, the United Fruit Company—whose dominance of the banana trade gave us the term *banana republic*—lost 234,000 acres of land. The UFC lobbied the U.S. government to oust Árbenz, portraying him as a communist puppet jeopardizing U.S. interests in the region. The idea of a communist foothold in that country was intolerable to the United States at the time. So, in 1954, the CIA orchestrated a coup, overthrowing the Guatemalan government. Secretary of State John Foster Dulles was a member of the law firm that had drawn up contracts between the UFC and Guatemala's dictator Jorge Ubico in the 1930s, and the Director of the CIA, Allen Dulles (John Foster Dulles's brother), served on the UFC board of directors. The Guatemalan coup became a chilling symbol of U.S. interventionism during the Cold War. While I'm sure the Dulles brothers and CIA field officers thought they were

doing the right thing to protect the United States from communist threats, it's hard not to see the dark tint of commercialism in the episode. Most of us today, including intelligence officers, would find ethical fault in this kind of intervention.

This history should show us what we did wrong and what we can learn from it. However, it should not make us shy away from the fact that the threats the United States faces today demand more, not less, economic intelligence. If we are to compete in a contested world, one where economic security is national security, the IC—as with Bridgewater and other hedge funds like it—simply must figure out better ways to collect, analyze, and share economic intelligence. The challenge is to figure out a way to do it while keeping true to American values, like maintaining a fair economic playing field and protecting privacy. This is yet another area where we can all, as citizens, have a say, take part in the debate, and make the right ethical choices that also protect our security. Whatever our consensus around economic intelligence, we require some level of it, because the alternative is a dystopian, authoritarian vision that certainly has no qualms about economic intelligence in any form.

★ ★ ★

To counter economic threats, decision makers must treat the issue for what it is, a grave danger to national security; and they must tell their intelligence leaders to get them the information they need to make better economic security decisions. Once agency leaders realize the threat, the focus in the world of intelligence will become collection requirements. These are exactly what they sound like, a list of requirements that are sent out to case officers and sensor operators like those controlling satellites. The requirements are ranked at different tier levels, and those tiers matter.

Think about it this way. When I was a case officer and sitting down to plan out an operation where I was going to meet a source, I would have to decide what questions to ask during a two-hour debrief. Two hours is not a lot of time, and I'm incentivized to ask the most important questions to get the best feedback on my intelligence reports, not only because doing so yields the best results, but because the outcome affects how I will be rated

at my job and, ultimately, whether I will be promoted. So, given that economic intelligence questions are rated as tier three, I'm most likely not going to get to those when meeting with a source, and I'll stick to my tier-one questions. Raising the requirement tier increases the chances of getting those questions asked and answered. Essentially the same thing goes for analysts deciding which reports to write. This prioritization goes for all new areas of expanded competition with China.

It's not all about more classified intelligence. To do economic intelligence well, you need economic information, and almost all of that is unclassified. Open-source intelligence is a key part of economic intelligence; indeed, it constitutes by far the majority of information you'd need to make decisions. The ability to acquire this data from commercial vendors, integrate it into intelligence analysis systems, and access it securely—all much more difficult than you'd imagine—is therefore crucial.

Additionally, you can have all the data you want, but if you don't have people who know how to make sense of it, then it's useless. If we want to do better economic collection and analysis, we need to have more and better-qualified people focused on the given issue. As a baseline, the IC must increase the number and quality of economics-focused intelligence officers. This means hiring more subject matter experts from commercial industry and finance, and that requires hiring those with MBAs and PhDs in economics, not just those who studied Arabic or international relations.

One problem with luring even the best financial wizards into the IC (a difficult task on its own, given the salary disparities) is that as soon as they leave their old jobs, their knowledge begins to grow stale. Staying relevant on esoteric commercial issues—from mortgage-backed securities, to how mineral spot markets work, to the technology and trade secrets of semiconductor manufacturing—requires constant updating. These experts must attend conferences, learn from consultants, and remain constantly engaged. For an analyst working in an SCIF all day or a case officer with a dozen other topics of interest, that can be impossible. Moreover, these analysts are generally limited in their ability to look at the U.S. side of the equation; they can't examine U.S. companies in the same way they can foreign ones due to privacy protections as well as legal and policy limits on

intelligence agency's ability to collect information on U.S. persons. Yet, to understand an industry, you need to understand all the players, including American ones. Solving for these types of issues requires rethinking how intelligence works at a more fundamental level.

When we look around for models for how we can do economic intelligence better, one that comes to mind is the Office of Commercial and Economic Analysis (OCEA), which was formed by the U.S. Air Force to work with other government agencies to assess economic risks to the defense industrial base. OCEA performed analyses not only of foreign economies and economic capabilities, but also of the United States' own supply chains and dependencies. Crucially, OCEA was not set up as an intelligence office. In avoiding the regulations that limit intelligence collection, it had unique flexibility in being able to work directly with market research companies and other commercial partners to collect information and perform analysis. Its reports informed Defense Department decision makers so that they can understand the economic and commercial challenges the country faces and make better decisions. This is economic intelligence without being economic intelligence.

Another issue for economic intelligence is information sharing. One highly alarming discovery of the 9/11 Commission was that terrorist information was not being shared among the CIA, FBI, and other agencies. Warnings about the 9/11 attacks slipped through the cracks. To help alleviate this issue, the National Counterterrorism Center (NCTC) was set up to share information and authorities across agencies on counterterrorism issues. Economic intelligence faces essentially the same problem as counterterrorism did before 9/11. Currently, the Department of Treasury, Department of Commerce, State Department, CIA, and any number of agencies may be focused on the same economic issue, but they will not share information with one another for policy and other reasons. Economic intelligence needs its own NCTC.

My take is that we need the equivalent of the NCTC for economic issues; call it a National Economic Defense Center, or NEDC, that would coordinate all governmental economic intelligence. In effect, the NEDC could maintain the equivalent of a real-time operations center for the global

economy, monitoring economic threats from China and other competitors and directing responses to those threats. They would exchange and analyze economic threat information, connecting dots that are not connected now and tapping into the deep expertise embedded across the government. Actions to counter threats would be coordinated across multiple law enforcement and national security authorities. The actors in this center would come from national security and civil agencies. This would mean the NEDC participants could focus on both domestic and international issues. The Departments of Commerce and Treasury would be obvious participants, but the center would also include agencies that focused on specific parts of the economy, from the Departments of Transportation and Agriculture to the Securities and Exchange Commission and Food and Drug Administration. Together with law enforcement agencies like the FBI and intelligence agencies like the CIA, this center could tackle the issue of economic intelligence holistically.

A major part of the NEDC, and any office facing these new asymmetric threats, is the need to bring even more open-source intelligence into the IC. For economic threats, this includes financial and commercial data and information from sources like Bloomberg or commercial satellites. Other threats, such as from science and technology advances, require their own forms of open-source information. This is a well-known necessity for the IC that nevertheless has remained a niche part of intelligence. There is an Open Source Enterprise, for example, which focuses exclusively on gathering and analyzing open-source intelligence. At the NGA, we had a program called Pathfinder, which used exclusively unclassified, open-source information to perform analyses. Some have even called for the creation of a separate open-source agency, one that would have the culture and technology necessary for the best possible open-source analysis.

But creating an NEDC or other open-source agency is just taking a page from the post-9/11 whole-of-government playbook. To truly tackle economic threats, and asymmetric threats more generally, the United States needs a new playbook.

Making the IC as good as a major hedge fund at economic analysis won’t work if you focus only on what the IC—or the government in

general, for that matter—needs to change internally. Neither the Intelligence Community nor the U.S. government will ever have as much or as timely economic knowledge as is contained within private companies. The economy is too big, the information too specific. Instead of trying to catch up, the U.S. government needs to bring in that outside corporate expertise. Economic threats demand that the public and private sectors join forces.

This is not unprecedented. In the late 1950s, the U.S. government had a similar issue of not having the best experts in science and technology. So it gathered a group of the best scientists, including several Nobel laureates, to perform summer studies for the DoD, the Department of Energy, and the IC. Since then, this A-Team of physicists, mathematicians, biologists, and others, known as the JASON advisory group, has performed classified research on topics ranging from nuclear weapons issues to climate change to LIDAR (light detection and ranging) to electronic warfare to Covid-19 risk. The same thing could exist for the commercial and economic sector.

As with JASON, a similar economic and commercial advisory group would be made up of the smartest, most experienced people in their field, from bankers with thirty years' experience doing cross-border transactions to the managers of the United States' largest ports. These are the people who know in minute detail how the economy and individual businesses work. They would not become government employees, though; indeed, the key stipulation is that they would continue to run their businesses. Rather, they'd lend their expertise to the government when necessary, answering questions and coming up with strategies or war game concepts of operation.

This is about more than just bringing in public-private expertise; the private sector must also understand the threat and take it seriously. Chinese companies are perfectly willing to forgo profit for geopolitical gain, something a U.S. company can't afford to do if it wants to survive. American executives will eventually come to realize that they must have a closer relationship with our government to survive economically, just as they do for cybersecurity threats. And though U.S. law enforcement already supports U.S. companies through an FBI-led public-private partnership called the Domestic Security Alliance Council, much more collaboration is required, given the enormity of the threat.

Indeed, company CEOs and other leadership may be in physical danger. In 2024 the United States and Germany uncovered a plot by Russia to assassinate Armin Papperger, the CEO of Rheinmetall, a German defense manufacturer. Rheinmetall was arming the Ukrainian military with artillery shells and was going to open a new armored vehicle manufacturing facility inside Ukraine. It appeared that there were also other planned assassinations as part of a larger program of sabotage the Russians had been carrying out across Europe in their quest to get NATO to stop supporting Ukraine.

CEO assassinations were once unthinkable, but they are now a very real part of the global economic competition. And while this plot was against an arms manufacturer, it's easy to see how the approach could spread to other strategic industries, like semiconductor manufacturing or mining. Indeed, just the threat of danger could have a chilling effect on economic independence. Intelligence can help stop these types of attacks—as it did in this case—but industry will need to work together with the Intelligence Community.

Information Sharing and Analysis Centers (ISACs) are one indicator of how industry and the IC might work together. ISACs are sector-specific organizations that gather and analyze information on industry-wide threats and vulnerabilities. They provide operational support and risk mitigation and facilitate information sharing between firms on specific topics. They also have threat warning and incident reporting systems for businesses.

In a model that borrows and builds upon the work that ISACs have done, companies, banks, investors, and academics would work together with the Intelligence Community to share information on economic threats and support economic growth. The concept is not unprecedented. There are programs that allow agencies like the Department of Homeland Security to share cybersecurity information with private industry. An order signed by President Obama in 2012, the National Strategy for Information Sharing and Safeguarding, outlined multiple programs for sharing sensitive cyber information with the private sector. Ultimately, the goal is to have the Intelligence Community share more threat information with U.S. companies to help them combat unfair business practices or even attacks on their businesses from adversary-backed businesses.

This brings us from a whole-of-government approach and toward a whole-of-nation approach to economic security. Our government and intelligence agencies would work together not only with one another but also directly with companies and corporate leaders to defend the nation. The Intelligence Community should be thought of as something more like an intelligence ecosystem, where actors in various domains coexist and operate together. There is no hierarchy but rather a web of relationships, where sometimes the actors cooperate (such as in a public-private partnership) and sometimes not. This is to protect all of us, because we are all under threat. The whole-of-government approach was a marker of the third intelligence revolution, and now this whole-of-nation approach is one of the key features of the fourth intelligence revolution. But even with a whole-of-nation approach, we may need a whole-of-planet approach to protect us from some of the biggest threats of all.

OceanofPDF.com

7

From National Security to Global Security

The disease tore through the city in southern China, forcing officials to shutter schools and send children home to their terrified parents. Travelers fled to Hong Kong in a desperate attempt to outrun the epidemic. With the Chinese health system on the verge of collapse, the army took over provincial hospitals. In one year, more than 160,000 people lost their lives. In response, the CIA set up a new program, Project IMPACT, to track the disease and Chinese military movements. This was not Covid-19. This was a meningitis outbreak in 1966.

Though this outbreak was naturally occurring, biothreats, not only born from terrorists or enemy nations but also harnessed from the natural world, are real—and the CIA has long known it. Since the early Cold War, the agency has operated intelligence programs to monitor and create early warnings for disease. For instance, Project IMPACT combined with Project BLACKFLAG, a CIA program that ran from 1968 to 1973 to "computerize disease information and derive trends, cycles and predictions." BLACKFLAG successfully monitored the outbreak of the deadly 1968 flu, even inside the closed borders of communist China and the Soviet Union.

We have all seen firsthand the threat posed by pandemics. Covid-19 killed more than seven million people, ravaged the global economy, and brought our social lives to a standstill. Other natural phenomena can also have devastating geopolitical effects. Earthquakes, droughts, and enormous storms can drive political instability across nations and even regions. The climate crisis threatens to become the biggest disruptor to human flourishing of all.

Yet if you asked most intelligence officers about their worst national security fears, these sorts of threats probably wouldn't be at the top of their lists. In fact, they wouldn't be on their lists at all, and not because they aren't a source of worry—we all had the same experience with the fear of the unknown at the start of the coronavirus pandemic. No, the reason is that most people within that domain don't see pandemics and other "natural security" issues as within the purview of national security. To most in the intelligence and military establishment, "national security" refers to threats like Russian invasions of Europe or Chinese aggression in the South China Sea. Pandemics, earthquakes, and the climate crisis are someone else's problem.

Unfortunately, this can no longer be true. Pandemics cause just as much damage as bombs. In fact, when measured in fatalities, Covid-19 was an atomic bomb's worth of damage. But more than that, diseases can be taken advantage of by nations for their own geopolitical purposes and so must be considered within national security contexts. At the extreme, diseases themselves may actually be engineered by foreign powers for such geopolitical aims. More broadly, other natural disasters, like earthquakes and the climate crisis, are becoming tools for leverage in the great power competition, with ramifications across all aspects of national security.

To account for this, we need to think more broadly when it comes to national security. We should include not just the political-military issues to which we are accustomed, but also other issues that affect the broader safety and security of the nation—and ultimately all human beings—and which adversaries may use to their advantage. Just as economics are becoming part of the national security game, pandemics, natural disasters, and the climate crisis are also now included—and so the rules must change. But it goes farther than this.

The United Nations, some nonprofits, and academics have begun to consider the concept of human security, which refers to security not at the national level but the level of all humanity. The idea is that any event that affects the health and safety of people, that creates fear and need, relates to security—and that the concept should apply to everyone, not just those who happen to be within your own nation-state. Accordingly, a concentration

camp or genocide in a far-off country is just as legitimate a national security issue as tanks rolling across the border in the next town over. This is a powerful, and controversial, concept.

Regardless of where you stand on human rights or climate change, there are pragmatic reasons to expand the conception of national security to its natural and human extreme. Pandemics, earthquakes, melting ice caps, and concentration camps are all threats and opportunities to nations that can and will be used for competitive advantage. Information about the spread of a disease may be hidden. A drought can destabilize a country to the point where a civil war starts. The ice melt in the Northwest Passage opens up new shipping routes to claim and defend. Human rights abuses are used to control and punish populations or, worse, to practice for more global ambitions.

Where national security goes, so goes intelligence. Decision makers face the uncertainty of the world and incomplete information. We sometimes get too accustomed to the idea of a free press that eagerly reports on the slightest natural disaster, but authoritarian governments regularly cover up such information. Disinformation may also be targeted around a natural disaster, to overstate devastation in order to maximize aid dollars, for instance, or to minimize fatalities in order to not show weakness to an enemy. Accurate information is necessary not only for knowing about the spread of a disease or the extent of destruction caused by a hurricane, but also so we can better understand the ramifications of these events, which range from the possibility of conflict, to the weakening of a nation's military industrial base, to how an adversary may use the event for opportunistic power grabs. Decision makers need this information as much as any other political-military information.

★ ★ ★

Covid-19 was as much an intelligence failure as Pearl Harbor or 9/11. The National Center for Medical Intelligence warned in November 2019 that the spread of a novel coronavirus in China's Hubei region could become "a cataclysmic event." The message was not heeded, and that is largely because our intelligence culture pigeonholes national security as a matter of

guns, bombs, and borders. While we might have seen it coming much earlier than the president's first mention of it in January 2020, we simply did not take it seriously enough. This isn't about whether a U.S. president comprehended what he heard in a meeting; it is no single individual's fault. It is about whether the IC as a whole took it seriously enough—and clearly it didn't.

One of the reasons we missed Covid-19 was that China appears to have hidden its spread. Chinese authorities squashed information about the disease, with, for example, information about its early spread being censored or otherwise not disseminated to global health organizations. This included when, for example, government authorities told the director of the Wuhan Central Hospital not to spread information about the disease. The more difficult thing to discern is why. As a *Foreign Policy* piece speculated, "It may have been a reluctance to cancel political meetings, a fear of public panic—especially around the Chinese New Year—the embarrassment of another pathogen being born on Chinese soil, or the simple instinct to squash bad news ingrained into officials in an authoritarian system. Pandemics are like wars. The first casualty is truth." This is precisely where the IC comes in, or should. Intelligence agencies specialize in rooting out hidden information. If given the mandate, they can do so in the case of diseases that an authoritarian government is trying to cover up.

Another reason Covid-19 and other diseases are hard to analyze is that we tend to see these sorts of biological threats as naturally occurring and random. In truth, diseases and their spread are not entirely unpredictable, nor uncontrollable. They are accelerated by population density, human encroachment on wild animal habitats, and the realities of an increasingly connected world that allows novel viruses and other diseases to spread around the globe in a handful of days. Sometimes these diseases can spread from lab accidents, as some have argued occurred in China. At worst, they can be spread on purpose, possibly through a bioweapon. Regardless of the mechanism, monitoring disease spread in general gets outside the comfort zone of intelligence agencies because it requires working with non-intelligence agencies and the scientific community.

Crucially, it’s not just about the disease; it’s about the ramifications. Covid-19 showed the world the power of biothreats in the way that Hiroshima did for nuclear weapons. Whatever its origin—a subject of much debate—the pandemic showed how much damage can be done by a disease. Millions died from Covid-19 and millions more from the effects it had on the health care system. The global economy contracted around 3.4 percent in 2020, wiping out a significant portion of the growth experienced over previous years—about the equivalent of a loss of two trillion dollars.

It also demonstrates how nations can take advantage of the destabilization caused by a pandemic. China used the excuse of Covid-19 to further implement tight control of its population and push forward its panopticon system. For instance, the CCP and its security apparatus sped up its process of tracking people’s movements, activities, and health status, assigning citizens a green, yellow, or red code that allowed them to travel or access public spaces. But after the pandemic, this system was not dismantled. Instead, it was extended farther, and also abused, with the issuing of “red codes” to freeze the bank accounts of protesters upset over a real estate construction project.

The Chinese government also used the smokescreen of chaos around Covid-19, while the United States and other nations were busy with their own internal affairs, to take control of Hong Kong and tamp down the pro-democracy movement there. It was no coincidence that emergency restrictions were extended in that city in early June 2020, despite only four people there having died of Covid-19 at that point. The anniversary of the Tiananmen Square Massacre is June 4, and the authorities wanted to stop any gatherings in remembrance.

No doubt, aggressive adversaries are taking note of how disease can be used strategically to benefit them. The intelligence failure around Covid-19 was not just about seeing it coming. It was about the failure of imagination to see what would be done once it was here.

★ ★ ★

It isn’t only about disease. Natural disasters can also create intelligence nightmares. The first climate war isn’t theoretical; it has already occurred.

In the years leading up to the outbreak of civil war in Sudan in 2003, desertification of historically pastoralist areas, combined with a lack of drinking water, caused a migration of people into historically agricultural areas, which caused disputes over land and water. When armed starving people come into contact with other armed starving people, the outcome is predictable. Between 2003 and 2008, about 300,000 civilians were killed, and about 2.7 million displaced. While still UN Secretary-General in 2007, Ban Ki-moon pointed out that the conflict in Darfur "began as an ecological crisis, arising at least in part from climate change." Others have noted the contributing role similar climate issues have caused in Syria, where a major drought in 2006–10 caused crops to fail and famine to spread in advance of the outbreak of armed conflict and civil war.

It's been said that geography is destiny. The climate crisis is quite literally reshaping the world's geography and, with it, our destiny. As Arctic ice melts, new shipping routes are opening up in the region. Melted ice can reveal resources that can be extracted. When things are worth something, they are coveted and protected. New potential shipping lanes require protection. The Arctic is becoming armed, with the United States, Russia, China, and other nations all significantly increasing their military presence there, from training marines to operate in cold weather to increasing submarine operations. Naval ships will need to take heed of changes in the salinity of water due to the melting of ice, which will affect where those ships will literally float or sink; this will require changes in their operations and routes. More unpredictable and powerful storms already regularly flood military bases and cause millions in damage, which affects military readiness.

Climate wars, changing geography, and the other effects of climate change will create many more national security ramifications, and the IC must provide decision makers with the information they need to understand these events. Climate intelligence, like that of biothreats, is not new. In 2009, the CIA set up a Center on Climate Change and National Security to analyze these issues. But this office was closed years ago, despite climate change being an exponentially growing threat to national security. It's time

that the Intelligence Community took climate seriously as a real national security threat.

The private sector, the government, and nongovernmental organizations responding to these events without the Intelligence Community is like fighting with an arm tied behind your back. Authoritarian nations are often unwilling to share disease data, or they actively keep outbreaks secret. The same is true of pollution or climate data, which may be controlled by a country for its own geopolitical purposes. This is some of the most important information that the IC, and the world, may need to mitigate natural threats. The Intelligence Community has the tools to get secret information and can use these to see not only missile movements, but also how diseases spread or ice caps melt.

But the biggest hurdle to understanding the intelligence ramifications of climate or pandemic threats is the secrecy not of adversaries, but of our own agencies. Climate change and pandemics are also scientific problems, and most scientific information is collected and analyzed by civilians and scientists. Intelligence agencies will need to work with the public on this topic, something these agencies are loath to do.

The climate crisis or pandemics or natural disasters can seem to be insurmountably complex, but there are many people who spend their lives trying to understand them. There are more than eight million scientists in the world actively involved in scientific research. The U.S. National Science Foundation estimated that global R&D expenditures amounted to almost $2.5 trillion in 2022. The National Science Foundation on its own had a budget of nearly $10 billion in 2023. There are close to four thousand universities in just the United States, and almost every single one of them has scientists on staff with their own research projects. Meanwhile, an intelligence office like the National Center for Medical Intelligence has around 150 employees. In other words, it’s civilian scientists who are going to understand these issues, not intelligence officers.

If it is to do its job properly, the IC must adapt to embrace these global scientists. To stay on top of issues, agency analysts need to access scientific information and use it for analysis, preferably before it is published, which can take months or years. Agencies need to hire more scientists who can

access, understand, and use scientific data. Part of this means working with other government agencies, including the Centers for Disease Control and Prevention's (CDC) Global Disease Detection Operations Center, which is charged with tracking and monitoring diseases. But it also means working directly with universities and other organizations that have no government connection.

A problem with this goal, to put it bluntly, is that many scientists do not trust the Intelligence Community and don't want to collaborate with it. They may consider themselves neutral when it comes to international politics. Or perhaps they have read about its past and view the Intelligence Community with suspicion or even contempt. They may also consider scientific information to be tainted if the information or scientists obtaining it come into contact with intelligence. And that's for American scientists. Scientists of other nationalities are likely to be even more distrusting of U.S. intelligence, if only for patriotic loyalty to their own nations.

Trust between the world of intelligence and the world of science will not be built overnight, but there are some things that can be done today. The Intelligence Community can do more to better explain why it should be trusted and how intelligence can help support natural security issues, from climate change to pandemics, a cause many scientists do believe in. More than that, though, trust is a two-way street. The Intelligence Community can and must begin to share its scientific information. That's not as outlandish as it sounds. In the 1990s, the CIA set up the Measurements of Earth Data for Environmental Analysis (MEDEA) program, which provided scientists with security clearances and allowed them to access classified information, such as historical satellite imagery, to use for scientific research. But the program was shut down in 2001. Restarting a similar program and sharing scientifically valuable intelligence would build trust and help not only the IC, but also the world.

There are examples of intelligence-like capabilities that could be a model for classified intelligence collection on natural security issues. For example, satellite images have been used to show mass graves in Iran and elsewhere, helping to gauge the impact of Covid-19. The U.S. government has declassified imagery from the CORONA program that has been used to

study climate change. Pollution data may not be available to the public, but perhaps a human source can obtain it from deep inside the Russian bureaucracy.

More broadly, government agencies can help in a whole-of-government approach. For example, the United States had a program to collect air quality data from embassies around the world, from Beijing to Delhi, and then release that data via social media. This provided real information to locals that may not be obtainable because their governments do not collect or share it. There were beneficial impacts to such programs. For example, once this data began to be released, one study showed how sharing air quality data from embassies improved local pollution. Imagine if the Intelligence Community could provide similar, but much higher-resolution or otherwise better, intelligence to scientists to further their research.

The world needs intelligence agencies and classified capabilities combined with open-source information to help battle these intractable natural security issues while also helping national security. Classified capabilities can also help civil society in human security or natural security issues, and they should be used to do so when their value outweighs the security ramifications. For example, the harm from declassifying CORONA imagery from the Cold War was negligible, because it was decades-old technology from a Cold War that is over, but it was helpful for civil society because such historical satellite imagery was not otherwise available. While declassifying secretly obtained information may burn the source, it might be well worth the trade-off to stop a genocide.

This is a vision in which the Intelligence Community is not only taking from the world but also giving to it. Again, this is not totally unprecedented. The CIA World Factbook has been made public, for instance, and does provide some public value. But imagine if even more products were made public and shared for the betterment of not only U.S. national security but also the world's security. There are pragmatic reasons to do so—it will help build trust with scientists and the public and may improve IC hiring. But there is also an ethical value for all of us. Sometimes intelligence is about not just a nation's people, but the world's people.

★ ★ ★

There is a saying that a single death is a tragedy, but a million deaths are a statistic. The same could be said of intelligence. One kidnapped American can capture the attention of a president and multiple intelligence agencies. But a genocide in Rwanda was of relatively little national security concern in the United States. This can no longer be the case.

Human security matters. While U.S. national security and the Intelligence Community are aligned in support of U.S. security, they haven't necessarily agreed on whether it is within their purview to ensure basic security for all human beings. Some members of the IC question whether general human rights should be a focus of national policy, and they argue that it would take away from more pressing domestic objectives. But even putting the morality question aside, there are very practical security reasons to consider human rights more globally. Human rights abuses often indicate other threats in a region and can tell analysts and decision makers much about the stability of a given nation or regime. Perhaps more important, and more cynically, abuses can create political upheaval and inadvertently cause ripple effects that lead to myriad security issues for our own nation.

After World War I, the idea of the League of Nations introduced the concept of human rights to the American public. The concept rests on the idea that individuals have innate value, regardless of their resident nation, and so deserve rights, regardless of where they are from. This idea of a global, humanity-level right to security was baked into the formation of the United Nations on October 24, 1945.

However, those UN human security ideals have not led to much intelligence on human rights. The United Nations does not have an intelligence function per se, and the United States has statutory limits on sharing intelligence with the United Nations—though there have been periods in which the United States collected human rights information. For example, during the Cold War détente in the 1970s, the CIA collected information on Soviet human rights abuses and reported it to the National Security Council.

In recent years, the issue of human security's relevance to national security has become inescapable. In December 2010, protests spread across Syria. Syrians, like many across the Arab world and throughout the Arab Spring, wanted to bring an end to the leadership regime in their country. These protests led to a civil war in which Bashar al-Assad, the Syrian leader, continued to commit atrocities against his own people. The United States and other nations were dragged into the civil war because of Syria's geostrategic position, its role in harboring and supporting violent extremists, and its stockpiles of dangerous chemical weapons. Human rights abuses, such as Saddam Hussein's gassing of the Kurds, were also one of the justifications used by the George W. Bush administration for the invasion and occupation of Iraq. These episodes show how human rights abuses can matter not only in themselves but because of what they can lead to.

As with scientific information, monitoring human rights requires working with the public, because most human rights and human security research is done by private nonprofits. Human Rights Watch is a nonprofit that investigates and exposes human rights abuses around the world. Other nonprofits doing this or related work include Amnesty International, Reporters Without Borders, and the International Crisis Group. But these groups are limited in what they can find out. Authoritarian governments want to keep human rights abuses secret. Indeed, they may not only keep these organizations out of their countries, but also threaten or even kill their own people to keep their human rights abuse secrets safe. Just as with natural security issues, human rights issues sometimes require classified intelligence capabilities to be fully illuminated.

As with scientific data in a competitive world, much about human rights is kept secret by authoritarian, and sometimes democratic, governments. Just as the Nazis attempted to keep their concentration camps secret, so, too, does China seek to keep its Uighur concentration camps as secret as possible. It has implemented programs to maintain the narrative that the massive compounds deep in the high desert are "reeducation schools" that so-called students attend willingly. These are blatant lies. In fact, these so-called schools are concentration camps where horrors occur

daily. The Chinese Communist Party has used its strict authoritarian controls over travel, the media, and the internet to make it very difficult to report on what's really going on in Xinjiang.

Intelligence agencies can help collect this information. Classified satellites and human intelligence sources could be used to better gather information on what is happening on the ground, while all-source analysts connect the dots. This intelligence reporting could be used to better inform foreign policy and to support outreach to allies with similar concerns. In some cases, the intelligence could be declassified to provide better information to the global public about CCP or other nations' atrocities.

Just as with data sharing between the IC and scientists, many in the nonprofit and human rights world do not trust the Intelligence Community. Also, similarly, trust must be built by treating information as a two-way street. The IC could share information on the human rights abuses it comes across. However, it may also want to purposely not share such information for fear it might inadvertently harm the abused people by associating them with intelligence. Consequently, in some cases, the IC may purposely choose not to do a certain mission, but instead just supply the tools for that mission.

Public-private intelligence partnerships are one way to work together where the IC could support a mission's getting done without inserting itself to do that mission. In one example, Tearline, a program designed by the NGA, shares intelligence information with nonprofits. It is designed for intelligence officers and others to collaborate on unclassified reports. The program allows users to write, edit, and comment on reports on various strategic, economic, and humanitarian topics. In essence, Tearline bridges the gap between classified intelligence gathering and public awareness. It uses publicly available information to create informative reports on critical issues. Through this initiative, the NGA helps organizations involved in thorny issues like authoritarian human rights abuses by showing them data and ways to use it.

Tearline is particularly important for supporting human rights analysis. The RAND Corporation used the NGA Tearline geolocation data and satellite imagery of Xinjiang's detention infrastructure to report on the

construction and expansion of preschool facilities for children and minors forcibly separated from their parents at Uighur reeducation camps. Another group, at the University of Texas, used Tearline to demonstrate how Russia was inflating Ukrainian refugee counts.

Such programs and reports are great examples of a public-private partnership between nonprofits trying to help the oppressed in the world and the Intelligence Community trying to protect national security. They allow policymakers to accurately understand what is going on inside China and, thereby, make diplomatic decisions. But this is also important information for Americans, and indeed the world, to understand. Combining an intelligence agency's data and analytical capability with non-intelligence analysts, keeping it all unclassified, and releasing that information makes possible the greater spread of better information.

It can seem pie in the sky to think about the CIA or the NSA working arm in arm with Human Rights Watch or a climate scientist, but it is worth considering for very practical reasons. What draws together a scientist, human rights researcher, and intelligence officer is that they all have a mission they believe in and want to accomplish. If they can better get that mission done by working together, it can be worth it. This takes building trust and ensuring that it's a mutually respected and sharing relationship, but there are examples of this happening. And with the world facing more and more complex challenges, all these groups may have no choice but to work together if they want to carry out their missions.

This is a hopeful vision for a whole-of-planet approach to intelligence that can be a part of the fourth intelligence revolution. It is a view where in the pursuit of global security, U.S. intelligence might have some very unlikely allies in human rights organizations and university scientists. It is admittedly optimistic, but we are not beholden to the past, where national security was very limited in its purview. Intelligence and national security will always be necessary to defend our nation, but they can also be used to help the world. We might call this whole-of-planet approach to national security the ultimate culmination of whole-of-government and whole-of-nation approaches. Though it might feel like the ultimate expansion of

intelligence, we are already expanding intelligence beyond the Earth, to the final frontier.

OceanofPDF.com

8

The Final Frontier of Intelligence

The greatest explorers have also been great spies. The two professions are intimately linked, with both spies and explorers illuminating the unknown. People like Sir Richard Francis Burton exemplify this connection. Burton's exploits and intellect are legendary. He spoke twenty-nine languages and led an expedition to Africa in search of the source of the Nile, becoming the first European to see Lake Tanganyika. But he was also a soldier and a spy, reporting back to the British Empire as part of the Great Game with the Russian Empire in Central Asia. Empires and nations need both maps and reports from the field. They must prepare for military contingencies or be able to make diplomatic decisions. Indeed, my former agency the NGA is charged with both making maps (the job of explorers) and uncovering what's really going on in those places (the job of intelligence officers).

This interplay between exploration and espionage continues today, even when the surface of the world has been almost completely explored. Now we've moved on to space. The Space Race was not just about putting men into orbit or landing them on the Moon; it was also about putting up spy satellites. Today, we are in the midst of a new space race, as the United States, China, and, to a lesser extent, Russia, India, and others put more and more satellites into orbit and push the envelope in exploration, from the Moon to asteroids to Mars and beyond. Intelligence follows this exploration and expansion, as it always has.

To see this race in action, just look up. On December 7, 2018, the Chinese launched Chang'e 4 (named for the moon goddess of Chinese mythology) into outer space and landed a probe, named Yutu-2, on the far

side of the Moon. This rover explored parts of the Moon the Americans and Russians never had. After first landing in the Von Kármán crater, a 110-mile-wide divot, Yutu-2 employed radar to explore beneath its surface. Because the Moon blocks the transmissions from Yutu-2 to Earth, the Chinese rover used a relay satellite to communicate with its base back home. And during all this, the probe remained invisible to U.S. observation.

While most Americans certainly missed this story, our intelligence agencies did not. No doubt, they were immediately aware of Chang'e 4's importance, not only for what it could do, but also for what its successful landing meant for our competition with China. Also frightening, the United States had no Earth-based means of tracking Yutu-2. Intelligence officers are a paranoid bunch, and they surely asked themselves what else our most capable competitor might be up to out there.

As the boundaries of exploration expand, so, too, does intelligence. The United States is already scrambling to learn what sort of space capabilities China has, what the CCP is building, and what China's real intentions are. It's not hard to imagine a future where clandestine intelligence and covert actions are undertaken on the Moon—if this isn't happening already. As things develop further, nations will spy on one another's lunar satellites and bases, trying to see what they are working on and who is there. Indeed, as soon as someone reaches Mars and begins setting up semi-permanent or permanent facilities, we will certainly see espionage become multi-planetary. Space espionage is not new; what is new are the players, the scale, and the distance we will go.

★ ★ ★

The era of spy satellites began with the United States' CORONA program, but just two years later, the Soviets launched their Zenit satellite program, which carried their cameras to capture pictures of Earth's surface and U.S. military secrets. Just as we did with our secret CORONA program, the Soviets claimed that Zenit was being used for scientific exploration, though it was of course being used for intelligence-gathering purposes. The Chinese successfully launched their first spy satellite, the Fanhui Shi Weixing, in 1975. The CORONA program ran through 1972, and the Zenit

program would operate into the 1990s. There were many more secret spy satellite programs on both sides, some of which continued to use film and, later, digital cameras, while others collected signals from antennas or other classified means.

From those small, very secretive beginnings, space-based intelligence has become a cornerstone of intelligence. The National Reconnaissance Office, which oversees building and launching spy satellites, has a classified budget. While there is little information about the size of the NRO's budget, the *New York Times* reported in 1994 that the budget was around $6 billion (around $12 billion in 2024 dollars). It's also safe to assume that budgets have gone up since then. On top of that, Space Force, the newest military service charged with organizing, training, and equipping personnel to protect U.S. interests in space, spent nearly $30 billion in 2024, and a large portion of that is devoted to intelligence. Space intelligence is big business.

By 2024, the U.S. government had around 170 civilian satellites and 250 military satellites in space. That may seem like a lot, but in that same year, around 10,000 satellites were operating in space in total, most of which were U.S. commercial satellites. Many of these commercial satellites are regularly used for intelligence purposes, as they collect imagery or other data that is then sold to intelligence agencies.

The future of space is commercial. It once took billions of dollars and thousands of people to put satellites and people into space, the work of a nation. Today, a high school team can put a tiny CubeSat into space for around the cost of a midsize car. That changes the game not only for space, but also for intelligence.

One company, the San Francisco–based Planet, designs, builds, and operates its own imagery satellites. The company was founded by former NASA engineers in 2010 and has since leveraged hundreds of millions in venture capital and, later, public market funding to launch more than two hundred satellites into orbit. Most of the Planet satellites are tiny (around a foot long), weighing less than eleven pounds. These satellites are launched on commercial rockets, and the images they take are beamed down to commercial satellite dishes around the globe. The images are then

processed in Planet's offices or in partnered analytical start-ups, where they are uploaded to the internet for anyone to purchase.

This sort of commercial imagery has accomplished something truly new, something the CORONA engineers could only have dreamed about. In 2017, Planet developed a system to provide an updated photograph of the entire world every day. To put this into perspective, while CORONA photographed approximately 590 million square miles of the earth's surface during its entire multiyear run, Planet photographs 186 million square miles every day. Now it is possible to shift from analyzing imagery produced in a single location at a single time to viewing the constant change of the entire world. And rather than being designed in a Top Secret military facility—literally, Area 51, used for the U-2—at the expense of billions of taxpayer dollars, Planet's doing it with around six hundred employees and hardly a security clearance in sight.

Nor is Planet alone. Other companies, such as BlackSky and Maxar, are providing their own electro-optical/infrared (EO/IR) imagery—that is, images in the visible and infrared light spectrums—commercially. Moreover, it is not just EO/IR imagery that is now available. Commercial company HawkEye 360 collects and processes radio frequency data from its constellation of satellites using advanced algorithms. In other words, it does commercial space-based SIGINT—something many of us in the Intelligence Community never thought possible. Capella Space, Umbra, and ICEYE provide synthetic aperture radar satellites commercially—another improbability is that there is not just one but multiple commercial SAR companies in the world.

After years of balking, the Intelligence Community is now embracing this commercial turn. In July 2017, while I was at the NGA, we signed a $14 million contract with Planet to purchase its imagery. It was in many ways a challenge to the NGA not only to sign such a contract—we were already spending hundreds of millions of dollars per year on imagery from DigitalGlobe at the time—but also to figure out what to do with all this new imagery. The system simply was not set up to look at the entire world every day. More than that, it was not set up to work with nontraditional, often venture-funded tech companies that were dual use—that is, they had

commercial products and ambitions beyond wanting to be government contractors.

Since my time at the NGA, the Intelligence Community has turned more and more to commercial space. The NRO took over the mission of acquiring commercial space imagery from the NGA and now has multiple contracts out for EO/IR, SAR, hyperspectral, and other forms of space data amounting to over a billion dollars. The NGA continues to acquire analytics from commercial companies to figure out new ways to analyze this data, using AI and other new technologies.

Commercial imagery isn't meant to replace the classified satellites; it is meant to be used alongside them. Classified spy satellites are the Ferraris of the space world. They are monstrous in size, highly intricate, and very expensive, but they do things no other satellites can. The term you often hear used to describe them is *exquisite*. They may have much better resolution or other highly classified features to better spy on adversaries. More important, they are secret, their full capabilities unknown to those we spy on, making it hard for those adversaries to defend against or avoid their gaze. But they are very limited in number, and their information cannot be shared with anyone who doesn't possess the highest of clearances.

Commercial satellites are much more inexpensive, much more numerous, and completely unclassified. This means they can capture more imagery at a lower cost, and that information can then be shared with anyone. With this imagery, a terrain map can be generated for use by urban planners, or a soldier can print a copy of an image and share it with foreign mission partners on the battlefield. This balance between the value of commercial capabilities and that of classified capabilities goes for many other types of "dual use" capabilities such as robotics or drones.

The biggest commercial space company of them all is SpaceX. Of the ten thousand–plus satellites in orbit in 2024, around six thousand were owned by SpaceX, part of its Starlink telecommunications network. Beyond satellites, SpaceX is best known for changing the game in launch with its Falcon 9, Falcon Heavy, and Starship rockets. These rockets were the first to be reusable and plunged the cost of a launch from ten thousand dollars or more per kilogram to around one or two thousand dollars per kilogram.

Eventually, they may get to one hundred dollars per kilogram, which starts being close to the price of a first-class airline ticket. This is a huge driver for bringing down the cost of the space economy in general and has been the opportunity for creating many other new space companies. Rocket Lab and other launch companies are doing the same.

The secret to their success is in thinking about space and space vehicles in terms of manufacturing scale. Rockets and satellites were historically mostly built in massive, sterile places where engineers in Tyvek suits moved cautiously around intricate components. When I visited the SpaceX headquarters in Hawthorne, just south of Los Angeles International Airport, it was the polar opposite—a chaotic jumble of activity as former automotive engineers built rockets at breakneck speed. It felt like they were racing to get to Mars—which, in fact, they are.

SpaceX is also getting into the intelligence business. In 2021, under its Starshield business unit, it signed a $1.8 billion contract with the NRO. While the details remain classified, the goal is to build and launch a network of hundreds of spy satellites—or maybe more—with specialized intelligence payloads into low earth orbit. As one NRO spokesperson said, this Starshield-NRO collaboration represents “the most capable, diverse, and resilient space-based intelligence, surveillance, and reconnaissance system the world has ever seen.”

The United States is not alone in this commercialization of space. The Chinese plan for space domination looks a lot like the way China came to control markets in 5G or rare earths. In 2014, the CCP opened the space sector to private capital, and in 2019 the China Commercial Space Alliance was launched to support that commercial growth both within China and globally. China’s space technology market is dominated mainly by the state-owned firms China Aerospace Science and Industry Corporation and the China Aerospace Science and Technology Corporation. It’s a safe bet that the CCP has already enacted a cyber intrusion and industrial espionage campaign to steal corporate and manufacturing information from the United States and space companies, including SpaceX. At the same time, China is able to harness its manufacturing strengths to produce less expensive satellites and launch capabilities. The Chinese government can then

subsidize these products for export through cheap central or provincial government financing. The space economy requires the same sort of economic intelligence as any other part of the economy to protect U.S. competitive advantage.

But this is not just a commercial space race. War is also coming to space. When President Trump first talked about plans for what became the Space Force, a new branch of the military designed to operate in outer space, some Americans thought it was a farce. Late-night hosts cracked jokes, memes proliferated on the internet, and Steve Carell even starred in a Netflix sitcom about the *Star Trek*–like operation. But many in the government knew this was no laughing matter.

When, on December 20, 2019, President Trump announced the establishment of Space Force at a speech at Andrews Air Force Base, he noted that "Space is the world's newest warfighting domain … Amid grave threats to our national security, American superiority in space is absolutely vital." This is equivalent to the formation of the U.S. Air Force in 1947, which led to a massive ability to fight wars in the air—from the B-52 strategic bombers prepared to fight nuclear war, to the F-22 Raptor stealth fighter jets that still maintain air dominance, to fleets of MQ-1 Predator drones to surveil war zones around the world. The formation of this new military service is the biggest signal yet that the United States is preparing to deter wars in space and, in the worst-case scenario, fight them.

Where war goes, intelligence goes. The Space Force also created its own intelligence capability and became the eighteenth member of the Intelligence Community. This includes Space Delta 18, which acts as the National Space Intelligence Center; and Space Delta 7, which is the intelligence, surveillance, and reconnaissance division of Space Force. Not long after, the NGA announced a change in its mission vision to note that it would "Know the World, Show the Way … from Seabed to Space." The agency in charge of making maps and looking at Earth is now preparing to do the same for extraterrestrial bodies.

One key mission of the Space Force is space domain awareness (SDA), which is focused on tracking and monitoring objects in space. With increasing space traffic from various nations and private companies,

keeping tabs on potential collisions and threats becomes crucial. Even small pieces of space junk (for example, leftover or broken pieces from space launches or nonfunctioning satellites) can have catastrophic effects. A softball-size piece of junk flying through space at 17,500 miles an hour could destroy a satellite or significantly threaten and potentially kill astronauts on the International Space Station. Moreover, with space being a warfighting and intelligence domain, there is a need to track military and intelligence assets in space, just as we track adversary submarines, bombers, and secret reconnaissance overflights. SDA involves a network of ground- and space-based sensors to create a comprehensive picture of what's happening in Earth's orbit. It is an innately whole-of-nation capability, with the Federal Aviation Administration and many commercial companies that provide data also playing major roles.

While tracking secret spaceships in Earth's orbit may sound like science fiction, it is already a day-to-day reality, and the future of space is even more outlandish. By the mid-2020s, NASA's Artemis program intends to return humans to the Moon. To complete this goal, NASA has teamed up with three companies, Blue Origin, Dynetics, and SpaceX, to design and construct aspects of the program. The goal is to create an operational Moon base. NASA has also let out contracts for building new Moon rovers and space stations, and some companies are already innovating in the areas of mining and construction on the Moon. Meanwhile, China and Russia have agreed to work together to create the International Lunar Research Station. The project aims to build a research base on the Moon for use by participating countries by the early 2030s.

The competition heating up between the United States and China, or the United States and Russia, will eventually expand beyond the Moon. Probes have already been sent to asteroids, and companies are planning to mine them for various precious minerals. The United States and, likely, China will send humans to Mars in the coming decades. And it's probable that SpaceX or other companies will meet them there, or maybe even beat them there.

Once there is real activity on the Moon or an asteroid or Mars, there will be intelligence there as well. Telecommunications will be necessary on

the Moon and other planets, just as they are on Earth. There might be radios used on the Moon's surface and communications satellites around its orbit. If there is communication, someone will want to spy on that communication. The United States and China will have bases and likely will want to keep some of the activities at those bases secret. So each nation will no doubt try to find out those secrets by using spy satellites or more secret means, like emplaced sensors. Even human intelligence will follow, as visual reconnaissance teams view what is happening in other settlements or try to recruit sources who live and work there. Intelligence has followed us from the Ancient Egyptians to today's modern skyscrapers, and it will follow us to the stars.

Space intelligence expands the world of intelligence to the farthest reaches. This is not science fiction; it is real. But intelligence will also remain close to us; indeed, inside us. And that might feel even more like science fiction.

OceanofPDF.com

9

Genetic Espionage

A young expectant mother prepares her first child's nursery, getting everything in order. She shows up to all her doctor's visits and couldn't be more excited. Like many of her friends, she's decided to get a genetic test of her child. Her doctor has recommended it—and *How could it hurt?* she thinks. The noninvasive test is approved across Europe, and millions of women have used it. This miracle technology in the comforting-sounding NIFTY test "can detect Down, Edwards and Patau syndromes and many other chromosome abnormalities and can also screen 84 microdeletion and microduplication syndromes."

This test is the brand-named product of BGI Genomics, a subsidiary of the BGI Group, a Chinese biotech firm with global operations. The test provides BGI with the genetic information about the fetus and the mother and other details about the mother's health and location. Perhaps she might find this innocuous, but many companies keep records of those who use their tests.

What should concern her, and all of us, however, is that BGI is not just another biotech company and that clients' genetic material is not being used just for patient tests. The development of the test was supported by the People's Liberation Army, and the genetic information obtained from the tests has been used in studies by the Chinese military. Her unborn child's genetic information is being used for research in many ways, including in the chilling-sounding area of "improving population quality." BGI has in fact been working with the Chinese military since at least 2010 to study the genomes of fetuses and newborns. It's also quite possible that the genetic

information is being secretly used elsewhere by the Chinese national security community, given that under China's draconian national security laws the company can be compelled to share any data it has.

The Chinese government has long had a mission of aggressively collecting genetic information on its citizens and others, using both legal and questionable means. Through the China National GeneBank, the CCP now has access to the genetic material of millions of people from across the world. BGI is a key source of the gene bank's data, as it is one of the world's largest genetics firms. Remember the grains-of-sand analogy? Why send operatives to another country to collect information when a company from that country can be welcomed in and, in fact, get paid to do it.

BGI is no stranger to controversy. It has been accused of a variety of illegal and unethical activities. In 2023, there were reports of its attempting to hack into Genomics England, part of the United Kingdom's Department of Health and Social Care, to access genetic data. BGI Genomics denies accusations that its information has been illegally or unethically obtained. The Pentagon and IC are aware of this and have stated that they see these activities as a clear part of China's initiative to grow its DNA database, to tap into new sources of valuable intelligence.

BGI and China's pursuit of genetic information is global. During the pandemic, BGI also aggressively marketed its Covid-19 testing kits and lab-based tests worldwide. It reportedly sold test kits to more than 180 countries and established labs in 20 countries. These labs were all collecting data, providing BGI researchers with access to personal information, health care data, and genetic information from around the globe. And as is part of the Chinese standard operating procedure, BGI acquired its technology through the acquisition of a U.S. company, Complete Genomics, which it bought in 2013, and a $1.5 billion investment by the China Development Bank (i.e., a CCP-controlled bank).

Meanwhile, the CCP has been systematically collecting the genetic information of millions of ethnic minorities in China. Human Rights Watch, in a great example of how nonprofits and intelligence agencies are now often concerned with the same issues, has reported that China has collected DNA samples, fingerprints, and iris scans for *all* residents of Xinjiang

between the ages of twelve and sixty-five. Furthermore, anyone considered a so-called focus person—code for anyone considered a potential threat to the CCP—has their information collected, regardless of their age.

When unable to collect information through businesses or its own laws, China turns to cyberattacks. In October 2023, a major U.S. genetics testing firm, 23andMe, was hacked. The data of between 5.5 million and 6.9 million users was affected. Hackers gained access to names, birth years, health data, genetic profiles, family linkages, and other valuable reports. Some of this information—for instance, about users with Chinese and Ashkenazi Jewish heritage—was then sold on the dark web.

Health insurance companies are hacked so regularly now that the news about another breach fails to shock. In fact, in 2023, one in three Americans had their health data affected in some kind of security breach. During that year alone, hackers targeted health providers and their vendors, infiltrating computer systems and exposing a record-breaking 133 million health records. These attacks weren't just about surveillance and disruption; in many cases, hackers demanded ransom or other payments. The frequency of these breaches is alarming, with incidents occurring every single day.

While U.S. intelligence agencies and law enforcement have linked China to health care information hacking, most people don't take it as seriously as they should. They've warned the public about the threat for years, though most people are unaware of the extent of the issue, as it is often lost in the seemingly unending list of data breaches to which we are constantly subjected. But this is different from having your credit card hacked or your Social Security number show up on the dark web. You can't just change your pin. This is your personal health information and genetic code.

This prompts us to ask what, specifically, is the value of all this genetic information being taken? Information gives competitors an advantage in intelligence, and biological information is another form of secret information that intelligence agencies will use for competitive advantage. For example, such genetic data could be used to identify individuals. Perhaps a nation wants to be able to identify whether a spy is in their midst when just a swab of DNA is available. Or they may want to use the

information to hack a personal, commercial, or government biometrics system. Maybe they could use the information to assess whether an individual has a genetic predisposition, preexisting medical condition, or mental illness, which could then be used to manipulate, extort, or blackmail that person. But there are even more disturbing cases. To understand the risks involved, we need to look at what is becoming possible in biology.

★ ★ ★

Increasingly, science and national security overlap, and the burgeoning field of synthetic biology is an example of where this is happening. Synthetic biology uses biotechnology to redesign organisms, giving them new traits or functions, or even creating whole new organisms. Since completion of the Human Genome Project in 2003, the science of genetic engineering has accelerated. New discoveries and approaches, including CRISPR-Cas 9 (a faster, cheaper, more accurate method of genome editing), have made it possible not just to map genes but also to modify them efficiently. Many of the uses of synthetic biology are truly revolutionary. They will save lives and bring about a better future.

Consider the work of Ginkgo Bioworks, a bioengineering firm that modifies living organisms for use in industrial applications, with a special focus on microbes. Ginkgo works with several industries, from pharmaceuticals to agriculture, engineering a wide variety of microbes that could be used as biofuels, to enhance food production, improve crop yields, create healthier food options, produce lifesaving drugs, act as targeted therapies, or clean up pollution or break down waste materials. One example is a microbe that produces nitrogen in the roots of non-legume crops that can’t fix nitrogen themselves, allowing these plants to obtain nitrogen from air rather than relying on its availability in soil. This could help revolutionize where certain food crops can be grown and in what quantities. We are entering an age when we can build new organisms as we once did new machines.

Ultimately, synthetic biology will change the world and do amazing things. Cancers will be cured. Sight and hearing will be restored. One company, Colossal Laboratories and Biosciences, for which I have been an

adviser, even wants to “de-extinct” the woolly mammoth, among other extinct animals. The idea of bringing species back from the dead was once the stuff of science fiction, but it is now a very real possibility.

However, this sort of research has also been used for far more profound and ambiguous purposes. In 2018, Chinese researcher He Jiankui and two colleagues modified the genes of human embryos to make them HIV-resistant. Doctors implanted them (they say unknowingly) into two women using assisted reproductive technology, with one mother giving birth to twins. He, who was sentenced to three years in prison for “conducting illegal medical practices,” insisted he wanted to protect the babies from HIV infection in adulthood. There is no doubt that He is not the only researcher pursuing such paths of inquiry; he’s just one of those we know about.

Already, synthetic biology is moving from government-sponsored labs to start-ups, and this knowledge will soon trickle down even farther. One place this knowledge will no doubt go is to college kids in their dorm rooms biohacking DNA, RNA, and whole organisms. Whereas once these tools were available only to massive government labs, with costs being driven way down, they will soon be available to nearly anyone. Just imagine smart twenty-somethings being able to create new organisms the same way they create new software today. This future is not far off and will no doubt lead to the same economic and social explosion of invention as occurred with the personal computer, the internet, and the cell phone. The trajectory of the technology feels very much like software and cybersecurity once did, which started with government labs and large companies and then trickled down to students and criminals. The ramifications of synthetic biology are also as dangerous as can be, as it is not just college kids with tech company dreams who will hack biology.

The South African bioweapons program during the apartheid era is just one example of how horrifying synthetic biology could turn out to be. In 1998, South Africa’s Truth and Reconciliation Commission investigated the apartheid regime’s Chemical and Biological Warfare Programme and its successor, known as Project Coast. Disturbing findings emerged, including that these programs developed lethal chemical and biological weapons to

target political leaders in the African National Congress and their allies, along with people living in Black townships. “These weapons included an infertility toxin to secretly sterilize the black population; skin-absorbing poisons that could be applied to the clothing of targets; and poison concealed in products such as chocolates and cigarettes.” They tried to make a weapon that would sterilize just Black people. In other words, it was a path to genocide.

That was forty years ago. Now imagine what synthetic biology could make possible. An authoritarian nation could create a genetically modified disease that sterilizes an entire population or ethnic group. And remember, the Chinese government has the genetic profile of nearly every human being of Uighur descent—it has already put one in ten of this ethnic group’s members into concentration camps. In some research, China has gone on to find genetic differentiators between Han Chinese, the majority ethnic group of China, and the Uighurs. Putting those facts together should drive a chill down your spine. Not only that, but China has also been systematically gaining access to millions of global genetic records from all sorts of population groups.

The implications of synthetic biology can sound even more like science fiction than that. Imagine an army of super soldiers, or even super geniuses. This does not sound so crazy when you consider the Chinese military research around “improving population quality” and know that BGI has worked with the Chinese military on projects to enhance soldiers’ performance. Yet it’s just as likely that scenario will not unfold as it does in the movies, with Top Secret programs developed deep within government agencies. Instead, because technology today is largely open source and available to all, there’s a good chance whatever is developed will soon become widespread, used by the military and civilians alike. The implications are hard to fathom. We assume certain constants in the human condition, but those assumptions are off the table if millions of kids are growing up with IQs fifty points above average and the strength and endurance of Olympians. Or imagine the social and political disruption of there being different classes of genetically modified individuals in the

world. Look at what sort of disruption has arisen from income inequality. Now imagine genetic inequality.

The dangers of synthetic biology cannot be understated. We should put it up there with nuclear weapons. The next arms race may not involve arms at all but living organisms. This new arms race might be about inventing bioweapons for use in warfare; or creating classes of super people; or terrorist groups using bioweapons to harm civilians; or about lone wolves biohacking any number of organisms.

Biothreats like these can feel overwhelming, and it's hard to comprehend how to stop them. But there are ways to mitigate threats. Consider the danger of dirty bombs. These are basically bombs with radiological material around them, so when they blow up, they disperse this material all over the place, irradiating people and places and, more important, instilling a lot of fear. This is a true terrorist device. So why haven't we seen such a device used yet?

The answer is both simple and profoundly complex: vigilance. The Intelligence Community works around the clock to prevent attacks before they happen, monitoring suspicious activity, tracking materials, and disrupting plots. This includes international cooperation with other nations' agencies to share information and patrol and surveil borders. The IC also invests in operations to collect intelligence and build relationships within communities to identify potential threats before they escalate. The list of prevented and thwarted attacks that we know about is long and impressive —and of course there are far, far more threats that the public will never be made aware of.

Dealing with something so revolutionary and full of risk as synthetic biology may mean doing two things: creating this level of vigilance and learning some lessons from cybersecurity. One concept is to treat biothreats like cybersecurity threats. In this view, every person, indeed every organism, is like an end point, to use cybersecurity parlance for computers and other connected devices. Each end point may be a target of biothreats, and so must be monitored. But the last thing we want to do is have intelligence agencies monitoring the personal biology and genetic information of every organism on earth. Therefore, we would need to find

public-private partnership ways to do this—perhaps one part personal doctors, one part nonprofits, one part voluntary use of new technology products. Such public-private partnership global vigilance could give us a heads-up when a new biological threat was detected. Scientists could then work together to halt the threat. It's just like in cybersecurity: Once a new computer virus is found, an update can be made to users' anti-virus software. The same can be true for literal viruses.

Global biothreat vigilance may mean that we need an entire intelligence agency devoted to biothreats—or, possibly a Biological Command (BIOCOM), parallel to Cyber Command (CYBERCOM), with the intelligence function to back it up. Regardless of whether it takes the shape of a large office or a new intelligence agency tailored to these threats, such a development would require new investments in this sort of intelligence, from new skill sets to new technologies. As with counterterrorism, this must incorporate a whole-of-government approach, including, especially, civilian health agencies. And if there were ever a need for a whole-of-society approach to a threat, it would be here. Companies, nonprofits, and civil society as a whole would need to play very big roles, as they did with Covid-19. This would require new public-private partnership pathways through a whole-of-nation approach.

We can go farther and imagine an international intelligence organization focused on tracking illegal genetic engineering and synthetic biology, whether in the creation of new diseases or the modification of humans or other animals and plants. Monitoring could then lead to international punishments and prosecution as well as attempts to find cures or reverse changes. We already see something similar with the World Health Organization and other organizations tracking global disease outbreaks, and in a sense, it would be similar to the way the International Olympic Committee works with the World Anti-Doping Agency to monitor and halt the use of performance-enhancing substances. Working together would involve incorporating individual nations, companies, civil society, and individuals. This would be, in essence, a global intelligence capability but one that was innately public-private and international in nature—a whole-of-planet approach.

★ ★ ★

Biothreats are one part of the much larger intelligence issue of how to monitor and understand breakthrough technologies. This is the job of science and technology intelligence, or S&TI. Strategic warning and avoiding surprise are core missions of the Intelligence Community. This includes science and technology surprises. Just consider the scientific breakthroughs of figuring out how to split the atom or to build an airplane that could go supersonic. These kinds of events are, in many ways, more important to intelligence officers and policymakers than coup d'états or invasions.

There is a long history of S&TI. During the Second World War, British and U.S. intelligence officers and military officers were aware of the superior technology and *Wunderwaffe*, or super weapons (wind tunnels, twin-engine diesel motors, rockets, and jets), developed in the Third Reich. To take advantage of the Germans' technological prowess in the aftermath of the war, the Joint Intelligence Objectives Agency was established to implement Operation Paperclip, which involved the contacting and recruiting of scientists from the collapsing German state. Operation Paperclip recruited dozens of scientists, and the United States gained access to invaluable German technologies, ranging from rockets to jet planes.

In particular, Operation Paperclip brought German rocket technology and scientists to the United States, including Wernher von Braun. Von Braun was the leader of the infamous V-2 rocket program. The U.S. government understood the value this technology could bring to weaponry and, eventually, the Space Race. Von Braun was initially transferred from Germany to El Paso, Texas, to form the core of a new rocket group. From there he was moved to Huntsville, Alabama, to begin work on the Redstone missile. Eventually, he was put in charge of the NASA Space Center, during an age of intercontinental ballistic missiles, reconnaissance satellites, and ultimately manned space flight. Today, von Braun is best known for designing the Saturn V rocket, which carried the first humans to the Moon.

China treats open-source intelligence as its INT of first resort, and in no area is this more so than S&TI. It's been reported that China has more than

one hundred thousand people focused just on open-source science and technology intelligence. Its intelligence system constantly probes secret technology development by the U.S. military and Intelligence Community, and especially commercial technology development. This information is readily transferred to Chinese companies, which go on to develop the technologies themselves and, more generally, better analyze U.S. military and intelligence capabilities to defend against them or copy them.

While the U.S. Intelligence Community remains great at S&TI when it comes to potential military threats, it is much less so for commercial or dual-use technologies. Intelligence agencies keep close watch over the development of new weapons systems. Important technologies like hypersonic missiles or new types of military sensors or next-generation submarines are tracked continuously and in detail. But when it comes to commercial technologies, most intelligence officers probably know about as much as the average reader of this book. They see the same news stories and read the same articles. The list of such technologies goes well beyond biotech to quantum computers, AI, electrification, and autonomy. Remember, the same rules apply as those discussed under economic intelligence: U.S. agencies are limited in what they can collect on U.S. companies, where most new technologies are developed. And even when there are foreign technologies that do pose a threat, like TikTok, we quickly run into the same morass of being unable to adequately collect data from and analyze these commercial companies and their products, because they involve U.S. users. This lack of knowledge of breakthrough commercial technologies can lead to technological surprise, in which intelligence agencies are caught unaware and therefore unprepared for new and potentially dangerous technologies.

ChatGPT is an example of a science and technology intelligence failure. This technology, developed by OpenAI, used massive amounts of data and compute to train a language model to essentially find, predict, and create patterns of words that would allow it to do amazing things, like write sonnets or explain quantum physics to a five-year-old or code software. There was no secret intelligence cell tracking the development of large language models like OpenAI’s ChatGPT that warned the president or the

director of national intelligence that this groundbreaking technology was coming. Senior-most intelligence officials were probably just as surprised as the rest of us when they first tried out ChatGPT and realized how powerful it was.

Luckily, this intelligence failure involved a U.S. technology, but it is highly likely that another such breakthrough technology will be developed by an adversarial nation at some point. Surprise breakthroughs in biotechnology in particular may come from China because that country has more lenient laws and social norms around experimenting on human subjects and otherwise developing technologies that may impact people. We could also see surprises in any of the number of other areas where China is rapidly improving in technology, from quantum computing to space technology to artificial intelligence. Indeed, when the Chinese AI product DeepSeek was released in 2025, concern flowed across U.S. national security circles that it might be a Sputnik moment, where China caught up with the United States on AI. DeepSeek was not quite Sputnik, but the next technology might be.

Science and technology intelligence failure is not always about missing the technology; it is often also about missing the consequences and ramifications of the technology. Contrary to popular belief, the Russian launch of Sputnik was not an intelligence failure. The CIA had been tracking Soviet progress, and Eisenhower knew well what was coming down the pike. Instead, the failure was the government's inability to imagine how the public would experience this Soviet achievement. Eisenhower and his cabinet did not anticipate just how much a Russian satellite in space would scare Americans. Similarly, the IC knew about Facebook and Twitter, but what they missed was how these platforms could be used for such massive and effective disinformation campaigns.

Maintaining an edge is not only a scientific or technological issue, but also a social, political, and economic one. It's about how the technology is used and its ramifications. The code intrinsic to Facebook, for example, was far less groundbreaking than the way people came to use it. The collection of our personal DNA matters far less than how the Chinese and those that follow will manipulate it. As technology plays an increased role in our

biology, and in all aspects of modern life, the IC must better understand and inform decision makers about all the implications of this technological change.

The IC must go even farther when it comes to understanding the present and future of technology—it must understand the nature of innovation itself to comprehend, forecast, and prepare for technological surprise. As with any other threat, if you are reacting once it has already happened, you are too late. The IC needs to see a technology coming so that it can provide time and space for decision makers to react to it. That means not being surprised. It means seeing what will be discovered, what will be invented, and what will be implemented.

The United States does have a historical model for analyzing and anticipating technological innovation. Developed under the Reagan administration, Project Socrates studied the decline of the United States' global competitiveness and offered a solution through more rationalized innovation. At that time, many U.S. policymakers felt that Japan was rapidly eclipsing U.S. industry and technology. The Project Socrates team found that in the aftermath of World War II, the United States began to shift away from technology-based planning and toward economic-based planning. Project Socrates began designing a system to collect and analyze information about innovation upon which it could then build an automated innovation system. The goal was to standardize the acquisition and use of new technologies to make the process much faster. The design also sought to pull the public and private sectors into harmony on innovation, making new technologies and their adoption into government and industry seamless. Though Project Socrates came to an end after President George H. W. Bush took office, the need for something like it lives on.

But for many reasons, the government alone is ill-equipped for this sort of analysis and forecasting. Just as with economic intelligence, predicting technological innovation is something that only current trained professionals, like venture capitalists, have any hope to do—and even those people fail more often than not. A public-private partnership would allow commercial companies to innovate data analysis, while the Intelligence Community could oversee its compilation with classified information and

recommendations to policymakers. A venture like this would demand highly trained specialists—possibly even an entirely new education and training program—and cutting-edge analysis techniques.

While the prospect of predicting innovation may appear outlandish, there is already a cottage industry of popular experts who try to predict innovation, like former *Wired* magazine editor Kevin Kelly and journalist Matt Ridley. There's also a history of developing new fields within the IC. During the Cold War, former OSS analysts developed the academic field of area studies as an outgrowth of OSS analytical approaches. The CIA funded and then hired from those departments to establish our modern approach to intelligence analysis based on country of focus. More recently, social network analysis went from being a niche academic field to a core intelligence analytical focus—and big business. It is possible to imagine the Intelligence Community funding the creation of innovation studies programs to support its S&TI mission.

The Intelligence Community can play a role in recommending how decision makers navigate innovation. Analysts could monitor private companies and recommend developing technologies for government funding. The Intelligence Community could likewise screen potentially dangerous foreign tech—say, a genetically engineered bioweapon—and recommend public and private solutions to curb new developments before they become threats.

Given an executive finding from the president, the Intelligence Community could even go so far as to try to covertly limit the development of certain technologies. This already happens with nuclear weapons, for example. During the Cold War, the U.S. government classified much of the technology behind making nuclear weapons. Intelligence agencies have also carried out covert actions to slow the development of nuclear weapons in Iran, by for example using cyberattacks to disrupt and destroy centrifuges or even assassinating nuclear scientists. In a sense, the U.S.-imposed limits on semiconductor exports to China are also an example of this, as they restrain the development of AI. These are examples of stopping the spread of existent technologies.

But if intelligence agencies could see the invention of new, dangerous technologies on the horizon, they could try to stop that technology's development before the invention occurs and spreads. For example, an agency might conclude that a new form of biotechnology could potentially be developed that would be very dangerous, and perhaps have little to no benefit to society. The agency might then try to covertly halt its development by, for example, recruiting relevant scientists to work on other unrelated topics, using information operations to change scientists' and entrepreneurs' minds about it, or, if it were in an adversarial nation, using sabotage to halt the technology's development. There could of course be overt versions of this, with for example the U.S. preemptively classifying information on the technology or the Department of State raising a global public awareness campaign about the danger of the technology. Such programs should only be pursued for the most dangerous technologies that almost all would agree create immense dangers while having little social value, on the same scale as nuclear weapons. But with technology being developed so quickly now and the potential for technologies that are as dangerous as nuclear weapons on the horizon, it may make sense for policymakers to have this tool available, even if only as a last resort.

We can imagine a program similar to Project Socrates for a new era in which the IC is charged with understanding and forecasting innovation in science and technology (S&T) and its social, political, and economic ramifications. This mission would be innately public and private, perhaps run outside the IC itself by federally funded research-and-development centers such as RAND or MITRE or through another nonprofit. The IC could provide funding and direction to these organizations. It could also support the mission of innovation forecasting by funding universities to build programs in the subject, just as it did with the field of area studies. But this would have to be done in an open, unclassified, and transparent manner. The value of monitoring innovation is one that accrues to all of us, as it provides time for society to debate, react, and adapt to the change. While most innovations are good, there are many dangerous ones, from biohacking to potentially destructive AI systems. An IC program focused on innovation could help inform not only policymakers but also the public.

This is another example of how the national security work of the Intelligence Community could help those in civil society who are also trying to tackle a global issue.

★ ★ ★

As nuclear power, rockets, synthetic biology, and other technologies have shown, new technologies breed new threats, and new threats breed new forms of intelligence. This is and always will be the nature of technological development. And that will not stop. Intelligence agencies have always tried to prevent technological surprise, but also to enlist new technologies. Such technologies, from satellites to submarines, have had profound impacts on intelligence. Today, we are faced with the progression of new technologies that are already changing everything we know about intelligence and that will drive the fourth intelligence revolution in fundamentally new directions.

Intelligence agencies have always been quick to invent or adopt new technologies. In World War II, the OSS thought to fit a radio inside a suitcase, making it possible to report back intelligence from behind enemy lines for the first time. During the Cold War, satellites were made to spy from space. It did not take long for the United States to ramp up a small program to mount cameras on the unmanned MQ-1 Predator into a 24/7 system of surveillance in two war zones after 9/11. The evolution of technologies like these also heralded revolutions in intelligence.

The Intelligence Community spends much of its budget on inventing, building, and using technology. Government contractors generally build these technologies, tailoring them to exactly what the IC needs. They even advertise. Stop at the Pentagon Metro station in Arlington, Virginia, and you'll see ads for surveillance drones, satellites, and other spy gear. As if developed by Q from James Bond, these technologies are sophisticated, fascinating, and cutting edge, but also utterly useless outside the world of spying.

After 9/11, the Intelligence Community began to turn to the private sector to use more commercial, off-the-shelf technologies. Some of these technologies had been initially funded by the IC, such as Google Maps,

which began as an In-Q-Tel program, and Oracle databases. (“Oracle” was reportedly the code name of a CIA program, the company’s first customer.) Today, the CIA and other agencies have cloud contracts with large hyperscale companies such as Amazon Web Services, Google, and Microsoft, same as most other large organizations in the world. Nonetheless, the average intelligence agency chief technology officer or chief information officer still spends most of their time modifying the commercial version of hardware and software to fit their tailored systems.

All these systems are for the essential purposes of securely collecting, analyzing, and disseminating intelligence. Satellites collect intelligence. Databases are used to store and access it. Analysts have tailored software for their job, whether that’s a geospatial tool to analyze drone images or a social network analysis tool to pick apart Al-Qaeda’s network. Technology is generally a tool for intelligence officers to use. As new technologies have been invented, they have disrupted intelligence and contributed to its revolutions.

Now two technologies in particular are driving the fourth intelligence revolution and will set the basis for the biggest intelligence revolution of all. One is artificial intelligence. All of us are witnessing firsthand how AI is altering how we work and play. This technology will have an equally profound effect on all aspects of intelligence, including calling into question what our role as humans will be in intelligence. The second technology driving the fourth intelligence revolution is the combination of information networks with the applications on top of those networks. These networks—from undersea fiber-optic cables to cellular networks to social media platforms—connect everyone in the world. But connecting us all means that there is now also a pathway toward more than just supersmart computers, seamless connections, and perfected surveillance. For these technologies and capabilities lay the groundwork for intelligence not only knowing all information, but also manipulating it. Together, these technology frontiers are profoundly altering our world and driving us toward the fourth intelligence revolution.

OceanofPDF.com

10

The Rise of AI

The massive twelve-wheel, camouflaged vehicle snaps branches as it drives over conifer-lined roads somewhere deep in the mountains of North Korea. It's a cold fall day, and early morning frost clings to the branches. The vehicle, a transporter erector launcher, or TEL, eventually pulls off into a grassy field where a small gathering of military officials waits expectantly. The driver and several others emerge from the vehicle. After some discussion and final preparations, a countdown begins in Korean—five, four, three, two, one—and the object that has been sitting atop the TEL rises slowly on a slant into its launch configuration, aimed toward the sky. It's a Hwasong-18, one of North Korea's newest intercontinental ballistic missiles, or ICBMs. The missile launches into the air with a deafening roar, spewing flames and smoke.

The Hwasong-18 has a range of nine thousand miles, meaning it can reach a target anywhere in the United States. It travels at over twenty thousand miles per hour, which makes it near impossible to shoot down and gives only minutes of warning. It's a solid rocket, meaning there is no need to fuel it, so as soon as the TEL's missile erects, it's ready to launch, which makes it very difficult, if not impossible, to blow it up before launch. The rocket can hold a nuclear warhead weighing over a ton, including a multiple reentry vehicle—the pinnacle of Cold War mutually assured destruction, where one warhead can split into many, striking multiple targets at once with atomic blasts. In other words, this is one very dangerous weapon that puts the United States at risk every day.

While this test fire ends up crashing into the Sea of Japan about 150 miles west of Japan's Okushiri Island, the launch definitely sends a message: if the world is going to enter a nuclear winter, it will be launched from the backs of these multi-axel behemoths.

What makes this all so hard for practitioners of intelligence is not so much the missile itself as the TEL. These vehicles start their life as Chinese-made road-mobile vehicles that can carry loads of up to eighty tons and range one thousand kilometers on a tank of turbocharged diesel. They were initially built to haul lumber or other construction vehicles, but the North Koreans bought and converted them—illegally, the Chinese claim—into missile carriers. While many Americans might be familiar with ICBMs, a TEL is something most people don't think about or even know to think about.

National Geospatial-Intelligence Agency analysts think about TELs constantly. Spend a few hours inside NGA headquarters in Springfield, Virginia, and I promise you'll hear someone mention a TEL at least once. And that's because TELs are some of the most dangerous tools in the world. They are hard to track, they're set up quickly, there are a lot of them, and, most important, they can carry nuclear weapons. It is one of the most important jobs of an imagery intelligence analyst to track the movements of these TELs. The fate of the country depends on it.

In the United States, our nuclear arsenal is a triad, involving ground-based nuclear weapon silos, air-based bombers, and nuclear-powered submarines that continuously circle the world. The U.S. approach to nuclear strategy centers on ensuring that, no matter what, we can get at least some of our missiles off the ground in immediate response should there be a surprise first strike. Knowing this, North Korea, Russia, and China increasingly use TELs, which gives them great mobility with their missiles, making them very hard to target. A TEL can be hidden in large garages or underground or even just camouflaged into the landscape. They can move on forested roads at night. They travel as fast as trucks and can keep moving constantly. Moreover, there can be dozens of them moving at once.

North Korean missile launches have thus far been tests. But the time may well come when the Supreme Leader sends a missile into a clearing in

the forest on the back of a TEL, fuels it up, conducts a countdown, and sends it flying in the direction of the American West Coast, hitting Seattle and killing hundreds of thousands or even millions of Americans.

The job of intelligence analysts is to anticipate and prevent such surprise launches. In this case, doing so would first involve finding indicators and warnings that North Korea was gearing up for a launch. Then and most important, they'd need to locate the camouflage truck in the massive mountainous forests of North Korea. From there, they'd have to deduce if the action was a test or a live launch, which involves keeping up-to-date about the North Koreans' capabilities and patterns. In the worst case, if it is determined that a live launch is about to occur, intelligence must give as much warning as possible so that those in power can do something preventative in response. These men and women stand guard with vigilance every day.

From popular culture, we're used to seeing spies land sources who reveal secret intelligence, thereby thwarting surprise attacks. But that just doesn't happen in a place like North Korea. In the film *Die Another Day*, MI6 agent James Bond attempts to infiltrate North Korea, only to wind up in prison serving a grueling sentence. Once his freedom has been negotiated by the British government, he does not return to North Korea—not in that movie nor in any other. This speaks to the reason spies don't often try to get inside the Democratic People's Republic of Korea: their chances of getting out again are not great. We also might hear a lot about open-source intelligence, but in a totalitarian state, there is little if any open-source information to pore over. Few pictures coming from North Korea make their way online, as cell phones there are rare and controlled. Thus, overhead satellite imagery is our primary tool for early warning when it comes to the "Hermit Nation."

Not long ago, an imagery analyst at the NGA would pore over stacks of developed film with a magnifying glass, hoping to spot a sign of something threatening. The advent of digital technology in the 1980s and '90s helped by giving these analysts digital images and high-powered computers on which they could scroll and zoom. But the work remained repetitive and

time-consuming because it still involved one analyst looking at one image at a time.

When looking at satellite imagery, the first order of business is to find the best images with the least amount of cloud cover. NASA tells us that about 67 percent of the earth is covered in clouds at any given time. Electro-optical imagery cannot see through clouds, meaning that there is a lot of looking at empty pictures. Alternatively, synthetic aperture radar (SAR) can peer through clouds, though SAR imagery is harder to interpret and has a lower resolution than conventional satellite imagery. With a useful image in hand, an analyst can look for missiles on launchpads, or for aircraft outside hangars, or for troops amassed for training drills. The analyst needs to find and identify the objects, then label and annotate them. This typically involves a series of choices and clicks from countless drop-down menus in specialized software. Doing all this with speed, efficiency, and accuracy takes considerable time and training—and this is only the most basic processing.

From here, the more sophisticated analysis can happen. First, is it in fact a TEL in the image? And if so, is it conducting an exercise or preparing for a live launch of a loaded nuclear weapon? Then, any other adversary activities going on, even far afield, are evaluated. This might give us indications and warning—for example, as to whether the adversary's leaders are nearby, prepared, and watching or concealed elsewhere in hiding. Other questions might be whether there are other military units mobilizing, what the pattern of life is for those involved in these exercises, and whether there have been deviations in that pattern. Ultimately, an analyst is asking him or herself whether the adversary is just pretending or if this is real.

Like all intelligence analysis, imagery analysis is largely an art of deduction: it's about connecting the dots, spotting anomalies, and drawing conclusions based on limited information. The stakes are high. Getting these questions wrong can spell the difference between life and death.

You would think that, in this life-or-death mission, the more data the better, but there are already far more images available than can be looked at by human analysts. On top of all the classified satellite images, dozens of

commercial companies are taking images with electro-optical, SAR, hyperspectral, and infrared sensors. The core problem is that the amount of data is overwhelming, and we could easily miss something and not connect one dot to the next.

This isn't a problem only for the NGA imagery analysts; it is a problem for analysts of all stripes. Ubiquitous surveillance means more data: more signals from more cell phones and more information from all manner of Internet of Things devices. More cybersecurity intrusions. More vulnerabilities, targets, and entry points than ever for bad actors. More social media and other internet data. Whereas the core problem of intelligence was once how to get information, it is now how to analyze all that information.

Indeed, the overabundance of data is a problem for all intelligence agencies, and it is a core driver of the fourth intelligence revolution. The NSA collects vast amounts of communications, electronic, and cyber data that no human could possibly hope to analyze. Similarly, the CIA and DIA collect immense amounts of HUMINT, MASINT, and other data. As the whole world does more and more online, the amount of open-source intelligence is scaling to inconceivable levels. As the fourth intelligence revolution requires agencies to look also at economic, S&T, biological, space, and other intelligence areas, it will require even more data to be processed and analyzed.

At the NGA, we had to find a better way to digest the hoards of data. The answer was artificial intelligence. Specifically, we homed in on a type of AI called computer vision. Think of computer vision as the visual part of human intelligence. It is about object recognition (what we are seeing) and change detection (how it is changing).

Computer vision gives computers the ability to see and understand the world around them. It is the driving force behind applications in a wide range of industries, including self-driving cars, robotics, and medical imaging. Not long before I came to the NGA, a professor at Stanford University, Fei-Fei Li, was instrumental in moving computer vision forward by creating a tool called ImageNet. This was a training set for machine learning (a form of AI in which the computer learns from lots of data) that

teaches computers to find and recognize objects and changes in images. Researchers using ImageNet data held competitions to see who would make the best computer vision system. The images used were totally unrelated to intelligence—typically, of different breeds of dogs. But the approaches and algorithms they developed could be applied to any problem, including spotting a camouflaged TEL in a North Korean forest.

We at the NGA recognized that AI like computer vision could change the game for analysis. These technologies can help analysts streamline vast amounts of rote work to arrive at the most impactful analysis. For example, the systems can remove all the images of the clouds or potentially identify and classify the different types of military vehicles in an image, completing one layer of work. This leaves analysts more time to connect the dots and ask the more fundamental analytical questions, like why something has changed or what the adversary's intentions are.

Artificial intelligence unlocks the possibility of being able to look at all the images all the time. Instead of an analyst receiving their workload from a satellite every morning and looking for changes, an AI system could constantly be analyzing every image that comes in so as to find any relevant change. The NGA could simultaneously monitor every forested road in North Korea looking for movements of a TEL—or in Iran, Russia, China, or wherever the threat comes from. Analysts could be alerted when there was a relevant change anywhere on earth in near real time.

Nor does it stop with images. Similar technology can be applied to SIGINT from military vehicles' electronic signals or the communications from Vladimir Putin or an ISIS commander, at any time of day and in near real time. Translation has historically been one of the most challenging obstacles for SIGINT and intelligence in general. Today, we are already entering a world in which any language can be translated into any other nearly instantaneously using AI. Patterns of activity could be analyzed around every case officer and their sources, with the AI technology remaining constantly vigilant for counterintelligence threats. All the new data from expanded intelligence operations in the economic, S&T, natural sciences, human security, and space domains could be analyzed as well.

Each form of intelligence requires tailored AI tools to help its process, from machine learning systems to run sensors to strategic-level intelligence systems that can produce all source products. It is computer vision for the NGA. Natural language processing and large language models can be used for communications, open-source, and human intelligence. Various forms of machine learning work on other types of intelligence. Some may be borrowed from the commercial world, such as by using financial tools for economic intelligence. Others will be made specifically to solve intelligence problems. Generative AI can be used across the board for summarizing and sense making around large datasets, as well as providing a human communication–like interface to hugely complex datasets.

Artificial intelligence can drive intelligence even farther into much more sophisticated forms of analysis. The technology can be used for modeling and simulation by creating AI agents that can model the thought processes and actions of adversaries. Scenarios can be planned and played out to see what will happen. Indeed, some have argued that China is already headed in this direction through the creation of parallel intelligence. In this approach, the Chinese surveillance system is used to collect as much open-source data as possible and then to model out the U.S. military, economy, and more to eventually develop countermeasures to our systems.

The U.S. military has long used modeling and simulation for technology development, but it is used relatively rarely in intelligence. That must change. As new AI agentic modeling becomes possible, in which AI "agents" perform tasks as humans might, the IC must adopt these groundbreaking capabilities. More generally, AI will allow intelligence officers to model many traditionally qualitative political science and international relations concepts. This will mean that over time social sciences will become part of an AI-driven model. Conceivably, the intelligence community could go so far as to model the world. Such a model could be continuously updated based on new data from sensors and other reporting, and provide a means to derive insights, perform scenario analysis, and even try out policies or actions in the simulation.

★ ★ ★

Artificial intelligence will do much more than just change how certain topics are analyzed; it will fundamentally transform the role of an analyst. AI isn't just another tool, like giving a carpenter a better hammer; it's more like providing a robotic partner capable of building an entire house. Since the beginning of modern intelligence, intelligence officers have used new technology tools—essentially better hammers—from mainframes to decrypt communications to word processers to type up reports to Palantir to find connections between terrorist suspects. But AI promises much more than that. Unlike traditional software tools, AI can learn and execute the same tradecraft practices as the analyst, in some instances, better than the analyst, allowing the technology to become a partner and collaborator. AI agents will be able to operate without human intervention, performing the entire analysis process on their own. Many of the tasks performed by analysts today, such as searching or labeling images or writing an intelligence report, can and will be done by AI. As AI capabilities grow, so too will its ability to conduct increasingly sophisticated analysis using more and more advanced tradecraft with precision and speed. This shift is not about helping an analyst analyze—it's about AI *doing* the analysis.

Yet rather than putting analysts out of business, AI will drive analysts up the value chain. It will enable even junior analysts to perform tasks traditionally reserved for senior experts or even whole teams. Consider the President's Daily Brief (PDB), a carefully distilled summary of the most critical intelligence, hand-delivered and briefed to the president and a select group of senior national security leaders. This consummate intelligence product demands hours of work by a team of hundreds across the CIA, ODNI, and other agencies. It is delivered by the most senior-level intelligence analysts in the government, who not only provide a brief but also provide context, explain the underlying dynamics of global events, answer questions, and take requests for follow-up reports or additional analytical products. These senior-level officials are super-empowered, coming into a meeting fully prepared by the best analysis and have immediate access to any information or outside experts needed. This privileged customer, the president, gets a perfectly tailored product that addresses what he needs, when needed. AI will super-empower analysts and

allow them to create bespoke PDB-like products for intelligence consumers far below presidents. One-star generals and senior government civilians or even lieutenants and junior civilians could receive such products.

The reason that intelligence officers will be able to do this is that AI will provide them with the time, space, resources, and capabilities to produce concierge intelligence. AI will allow any analyst, even junior and mid-level ones, to harness the vast expertise of the intelligence community and tailor a customized report for the specific needs of their customer. They could focus on managing the process and the AI, tasking it to analyze what is necessary for the briefing, and then interpreting that information for the customer on the spot. They'd act as the critical link between various forms of intelligence, piecing everything together while also acting as the editor and the spokesperson. Ultimately, instead of being just briefers, intelligence officers would evolve into true partners with their customers, working collaboratively to support the best decision making possible. In the end, analysts could have the time to really get to know their customers, similar to how a concierge doctor, who has a tenth as many patients, can deeply get to know their patients and treat them in a high-touch capacity.

More than just having more time, all analysts will become super-empowered by AI. Analysts will originate ideas and identify critical issues, delegating AIs to take a closer look, much like senior analysts or managers might do today. For example, the analyst might have a hunch about a counterintelligence issue and then could have AI agents check thousands of sources or process millions of data points to find patterns. Instead of pursuing one lead, he might pursue hundreds or thousands simultaneously. Their focus will shift to high-level problem-solving, critical thinking, and developing innovative solutions, tasks that are currently among the most valuable aspects of an analyst's role but often receive less attention due to the time spent gathering, processing, and performing routine analysis (or, for those more senior, managing others). When AI can handle these tasks, analysts—even at the junior level—will have the bandwidth for higher-level job functions.

Being a super-empowered analyst will be more like being an entrepreneurial CEO. The analyst will provide a vision and overall strategy

for what must be done and then delegate tasks to those who work for him; in this case those being delegated to are AI systems. For example, an analyst pursuing a goal of tracking down a terrorist could leverage multiple AI tools to produce comprehensive intelligence on the target (just as a senior analyst might leverage multiple junior analysts to do now). The CEO must still think critically, as he may be presented with questionable information or a change in the environment. He can then course correct his subordinates or even go down an entirely different path, such as creating a new product. When things change enough, he can pivot his vision or strategy to suit the new environment. The super-empowered analyst might pursue multiple lines of inquiry at once, checking back with the tasked AI systems periodically to see if they've come up with anything. A single human analyst would likely be able to accomplish what dozens might accomplish today.

One key skill of the super-empowered analyst, and any user of AI, can be likened to the art of curation mastered by those who run fashion boutiques. With so much information and analysis at their disposal, intelligence officers will need the discernment and "good taste" to decide the most relevant and valuable insights for their specific customers. By deeply understanding their customers, much like the director of national intelligence builds rapport with the president, analysts could tailor not only the content of the intelligence they deliver but also its format and presentation, ensuring it aligns with their customers' preferences, requirements, and cognitive style. For example, President Reagan liked his PDBs delivered as television shows, whereas President Obama wanted to interact with the information on an iPad. President Trump reportedly wanted more economic information in his briefings. President George W. Bush was given deep-dive briefs on specific topics that often turned into policy development sessions. A super-empowered analyst would have the bandwidth, freed up by AI, to focus on refining these issues of taste. Furthermore, an intelligence consumer might not always know what to ask for, and an analyst can help guide them in identifying their needs. A concierge analyst could teach their customer how to effectively utilize intelligence and discern what to pay attention to. They also have the

expertise to select the right tidbits of intelligence and present information in a tailored manner.

This won't just be for analysts; other types of intelligence officers will be super-empowered by AI. For example, case officers could delegate AI systems to prepare their surveillance detection routes, find overlooked patterns in their cover stories, search out counterintelligence issues, or otherwise gather data and information that takes huge amounts of time today. They would have the time to think even more broadly about their mission, coming up with a vision for operations in a country that they execute across several forms of intelligence, tasking satellites or other sensors and running sources. It is more like the level at which a chief of station—the senior-most intelligence officer in a country—currently operates at.

Being a super-empowered analyst is a radically different role, compared to the traditional image of the analyst profession, and that's exactly why this marks an intelligence revolution. These are not minor changes to how intelligence operates; they're fundamental shifts. It requires rethinking everything. That means hiring different types of personalities and training people differently. Promotion will change as people are rated based on different aspects of their work. Ultimately, the entire workflow and system of intelligence will change as the current structure, which is essentially based upon a bureaucracy of people, will need to adapt to a new system in which much if not most work is done by AI machines and humans become the managers of these machines.

★ ★ ★

AI is the game-changing technology for the fourth intelligence revolution. Over the last several decades of intelligence in the United States, we increased, year after year, the collection of data. We first grew intelligence agencies to handle it all. Then we developed computers and analytics to help those analysts. But new technologies have grown a data collection that is so large, humans and tools can't keep up. AI is the only choice to overcome this challenge. While technology is the creator of much of this tsunami of data, it also provides the solution.

The competition between the United States and adversaries is driving the adoption of AI in the fourth intelligence revolution. Vladimir Putin himself said that “Whoever becomes the leader in this sphere [AI] will become the ruler of the world.” But all pale in comparison to China. The CCP is explicitly trying to become the world leader in AI and, specifically, to use it across its intelligence and national security community. China’s intelligence revolution is driven by attempts to collect data on all people, and to analyze all this data, the Chinese must use AI. It is their intent to lead in AI to maintain a competitive advantage. We must do the same or lose our own competitive advantage.

It is imperative that the United States adopt AI for use in national security, especially in the Intelligence Community, but the road to doing so couldn’t be more difficult. Coming up with the insight that AI can help solve the Intelligence Community’s problem of too much data or that analysts should become super-empowered entrepreneurial CEOs is straightforward. The real battle is implementing this groundbreaking technology within the slow-moving, complex, bureaucratic labyrinth that is the U.S. government.

OceanofPDF.com

11

From Augmenting to Automating Intelligence

Imagine you're sitting at the desk of an NGA imagery analyst. Perhaps there is a framed family photo and a cup of stale coffee, as at any desk in any other office. But unlike desks in the outside world, there are also multiple monitors, connected to multiple computers—one that is on a Top Secret–classified network, one on a Secret-level network, and a third on the Non-classified Internet Protocol Network, or NIPRNet, a network secured by the military.

When one turns on the monitor, the software looks old and blocky compared to what's on the analyst's cell phone (stored in a locker outside the building). This software was designed by one of the world's largest government contractors five or ten years ago, based upon a series of requirements that a bureaucratic process came up with a year or two before that. The analyst has no choice but to use this software, and any feedback he has on how to improve it would take years to be implemented, if it's listened to at all. Perhaps the analyst's supervisor has promised that there is a "fair and open" contracting process under way to update the software, but that's been the story for the last two years already. The analyst is not hopeful.

The data this software runs on comes from satellites and other classified sources, which are magical in their capabilities but very limited in their availability. The analyst can request new data of the same type through an involved, multistep process, but often his requests go unheeded, as they are trumped by someone else's requirements. Under no circumstances may he get any data that does not fit the standard parameters. Hopping onto the

internet, googling a new data source, downloading it onto his computer, and working with it would be tantamount to treason. He would be not only investigated for doing so, but possibly fired.

The analyst must stick to the standard workflow he learned during a course he took when he was hired eight years ago. The software and data are functional, and with them, he can accomplish his mission. Every morning he sits down at the desk, there will be new batch of data to analyze. His performance rating will be determined by the quantity of analysis he performs as well as its quality. While there is some room for critical thinking and creativity, oftentimes the work is so unceasing and overwhelming that there is no time.

The process can feel oppressive and unyielding, and it is, but the work is important, and the analyst is driven to succeed. He knows that if this job doesn't get done, bad things could happen in the world. Perhaps a TEL slips by unnoticed on that one day North Korea decides it's no longer bluffing and wants to actually attack the United States. This is the analyst's nightmare. So he remains obsessive about accomplishing his mission. If anything, over the years he starts to grow untrusting of any new technology that is offered to help him accomplish his mission. He's been promised new tech, but often it doesn't get out of research and onto his desk. He's seen people try new software before, but it always seems to be so fragile and not work well. He knows one thing: how to do his job within the system. Clunky and slow as it might be, it has worked, so far.

But every day, it feels like there is more data to analyze. And every day, it seems like there are more threats to be concerned about. And every day, the adversary's tradecraft is getting better. Something must give.

When, one day, an unusually young-looking senior leader gives a speech about how AI can solve the analyst's problem, it seems too good to be true. The analyst is skeptical, if not cynical. Artificial intelligence seems like the Kool-Aid everyone is drinking these days. But there are so many challenges. This AI was developed by companies with no experience with classified systems, and that might be insecure. The contracting process can take years, by which time the AI might no longer be on the cutting edge. The AI does not fit into the analyst's current workflow. It's not clear how he

will be rated if the AI does much of the workflow on its own. And if this AI does somehow miraculously make its way into the agency and work as well as is hoped, perhaps he is more secretly concerned with what will happen to his job. But more than any of that, this AI is simply not as trustworthy as another analyst. It's not been tested in the real world over time. The mission might not get done, and that TEL might slip through the cracks.

These questions were just as real when I was at the NGA as they are today. They're legitimate questions, and there are no easy answers. But, in the end, AI will be necessary to maintain a competitive advantage. Though we did not call it the AI-driven fourth intelligence revolution at the time, we saw this need while I was at the NGA, and there are some lessons to be learned from our experience of trying to bring about that revolution.

★ ★ ★

The National Geospatial-Intelligence Agency, like many national security agencies, had already been working on AI for years when I came along. The problem was that the AI was not being integrated into operations. Typically, it was the Research group within the NGA that was focused on AI, and they had developed many good systems for computer vision. In parallel, there were commercial capabilities coming out of Silicon Valley that could be used for the NGA's mission. In-Q-Tel brought some in, and others we found ourselves, particularly after we set up an office in the Bay Area. To support this transition, we ended up creating the Office of Ventures and Innovation. This office's mandate was to use a design methodology to fully understand the problem to be solved with AI or data, to figure out how to implement the technology, and to help nontraditional companies bring their technologies to the NGA. Many hard-charging, initiative-taking officers, especially in the office of Analysis, also figured this out on their own and began their own AI analysis programs. To keep all these AI-related moves straight, I created a new role and appointed the agency's first Director of AI, Automation, and Augmentation (AAA), the first position of its kind in the Intelligence Community.

Once found, new technology must be acquired and integrated into operations. At the NGA, we had to set up new means of acquiring

technology from small tech companies, some with only a few employees. These were companies that had never even heard of the arcane Federal Acquisition Regulations, the dreaded and often derided FAR, a document of over a thousand pages that governs how the NGA and most Department of Defense and intelligence agencies manage their acquisition process. This included using the vaguely, if aptly, named Other Transaction Authority, as well as Small Business Innovation Research (SBIR) grants, and sometimes simply offering personal guidance to new companies. At one point, we even tried to trade our data for AI algorithm development in a public-private partnership—a partnership approach that I still believe in but which was too radical at the time. We also needed to figure out how to incorporate this new technology into the existing, massively complicated software systems that analysts and others used by working with the contractors who built those systems, a problem that persists today.

However, finding and acquiring the technology was not the hardest challenge; the hardest challenge was figuring out how people would work with these new AI tools. My approach was not necessarily to teach everyone to code, but rather to teach computational thinking—that is, the ability to solve problems using scalable computational methods. We still require subject matter experts, whether on the culture of a specific country or military strategy (or finance or human resources, for that matter). But how they solved problems in their field could also incorporate computational methods, including AI.

We started by teaching the programming language Python, which is often used for data science, to understand how to work with data and AI. One of the students in the first class was our director Robert Cardillo, who took the class seriously; he even wrote a program using Python in it. Perhaps it may have been the first program written by any sitting intelligence agency director. The point wasn’t for him to code, of course, but rather for him to show that computational thinking could help even a director understand and solve problems. After a while, the agency developed a tighter curriculum, one that focused more on computational thinking and less on coding per se.

While everyone needs to understand computational thinking, we also need specialists. In 2017, we started Data Corps, an NGA office staffed exclusively by data scientists, data engineers, and similarly highly skilled technologists. These were experts who could work with the NGA's analysts and other data users to help process all the new streams of incoming data. Creating the Data Corps was a lesson in what is possible in the government world, where many feel that hiring new technologists is hopeless. When we sought to create the group, the NGA had fewer than ten full-time data scientists, with a 25 percent turnover rate. Within the first year, we filled all eighty-five billets for the program, including an outstanding chief data scientist. The lesson learned was that technologists will serve in government, as long they are given the most challenging engineering problems and the freedom to build and work with technology.

An irony for AI is that the technology is now bringing us toward a point where people do not need to learn to code and, in fact, soft skills may become much more important. AI systems like large language models already support software development, and in the near future most coding will be done by these AI systems. The role of human developers will be more like being an architect, telling the AI what to build, and stressing the artistic rather than engineering side of architecture. This I believe will shift the valuable skills toward more creative training, such as the arts and humanities, even (and perhaps especially) for those developing software.

Progress was painstaking. But we did continue and accelerate a process that had been ongoing since the first intelligence revolution, of implementing new technologies to solve intelligence problems. Decades before, it was working with radar or the first satellites or the first computers. This time, it was figuring out how to use new datasets and implement AI. Changing technology also means culture and assumptions need to evolve. When I was at the NGA, I had a simple vision that AI would help people analyze the data, but today it can do much more than that.

In 2022, seemingly out of nowhere, OpenAI launched ChatGPT 3.5, and it caused just as much of a frenzy in intelligence as it did in the commercial world. Suddenly, this technology was more than responsive; it was creative, moving into areas we had long thought of as distinctly human.

People used ChatGPT and similar large language models, or LLMs, not simply to get answers to questions, as they do with Google. They used it for much more, such as to help rewrite an email or develop a logo or tell a fictional story or any number of creative, complicated things we once believed only humans could do. It's as if the AI moved from our more reptilian brains (describe what's in a picture, perform basic translation) to our frontal cortex (be creative and thoughtful).

Many of us in the Intelligence Community realized that this innovation had profound implications for the work we did. AI has the potential not only to be a tool, but to be a true partner. When we asked NGA analysts what they wanted from AI, they often mentioned J.A.R.V.I.S., the AI assistant from the *Iron Man* comics and movies. The idea is to have an assistant who could help with projects, whom you could ask a question of or direct to do something, like pull all the data on a given topic or run an analysis. That was still science fiction while I was at the NGA. Today it is real.

The key concept is human-machine teaming, and there are multiple ways to do it. One is to have machines as a tool. This is how we use Google search and related software systems now. Many of us use Google to help us recall information—by searching our email, for example. In effect, software is a tool and is acting as an extension of one's memory in this situation, just as a shovel is a tool that extends our hands to lift and move dirt. As one starts to move into the world of advanced analytics and AI, the human-machine teaming becomes more complex. The machines can perform some narrow tasks on their own while we still perform the bulk of the work. The sort of computer vision object recognition and change detection we worked on at the NGA were in this category, where specific narrow tasks could be assigned to the machine. The system might also be narrowly predictive of our inputs—for example, by recommending how to complete a sentence as we write. This is still a tool that requires a human to operate it, but a much more advanced one.

The next-level approach is more like J.A.R.V.I.S., where we have an AI agent that can act on its own. In an agent model, an AI-driven analytical system might perform its own analysis in parallel with a human. The AI

could tackle different aspects of the same problem. Perhaps it would perform actions that machines were better at, like finding and processing data or statistics, while the human could perform more reasoning-based analysis. Or the machine analysis system could independently develop alternative scenarios, which the human could use to compare with his or her own analysis. In the most advanced state, AI agents go so far as to gather data, analyze it, and write a report on their own. Humans then might perform quality control and insert more advanced reasoning, context, and creativity. In this scenario, the AI is more like a teammate than a tool.

Human-machine teaming is not just an analytic strategy. HUMINT officers benefit greatly from it as well. For example, an AI approach could help case officers find hidden patterns in their surveillance detection routes or communication plans that they might not be aware of. This sort of automated data analysis of operations is particularly important when we remember that our adversaries will be performing their own pattern recognition using their own algorithmic systems and seeking such patterns. The only way to even the odds will be to have such tools. Indeed, this is especially necessary as the world becomes ubiquitously surveilled. This human-machine team could work to discern complex patterns, monitor ever-present sensors, and otherwise work together to overcome this complex problem of finding hidden patterns in surveillance, communications plans, or other HUMINT operations.

It’s important to mention that in no way does the suggestion of human-machine teaming question the innate value of traditional human capability, especially when it comes to intelligence. Qualitative, social science, or humanities-based approaches and more generally intuitive and creative thinking are exceedingly important in all aspects of intelligence. An illustrative example is Alphabet’s Jigsaw company, a technology incubator that tries to apply technology to global challenges. Jigsaw had a program to combat disinformation. Using a strict data science approach did not work. Instead, it brought in anthropologists to spend time talking to conspiracy theorists to learn how they thought. In doing so, the company learned new things—for example, that slick, expensive-looking websites were less

trusted because they were considered part of the “elite” system. Human-machine teaming like this is the vital approach.

More generally, AI approaches to analysis are rife with pitfalls. Models are fragile. This is particularly the case with machine learning models, which tend to be extremely narrow in focus and can easily produce poor results if asked to do anything outside the focus area or if the data is slightly off. Lots of context is necessary to understand what is going on in the world. Reasoning is necessary to work through complex problems. These are things that AI has yet to master. In contrast, humans are extremely flexible and good at spotting patterns, bringing in context, and applying reasoning. There is also a problem of hallucinations in large language models, where these models make up data or information that doesn’t exist.

These pitfalls can be overcome, and I predict that, soon, well over 90 percent of intelligence will be made by or for AI systems. AI-derived sensor systems will collect much more data, as for example autonomous drones proliferate or AI agents scour the web. As more and more data pours in and as better AI becomes available to process that data, it will be only natural to have the AI process the data. This percentage may sound high, but then again, if someone in 1965 had been told that, soon, 90 percent of intelligence would be processed on a computer, that might have sounded high. Today, 100 percent of intelligence is processed by a computer at some point. Not only will 90 percent of intelligence be automated, but it should and it must if we are to keep up with threats, just as we would have no hope to keep up with threats today if we still relied on paper files and mailing letters.

The biggest problem to overcome in adopting AI is trust, and it remains the hardest part of human-machine teaming. In intelligence, we gain trust in people only by understanding how they are trained, seeing them in action, and ultimately spending time with them. We want to know how they think and to be sure that they are trustworthy and good at their job. But the days are dwindling when a president can simply call in the analyst who spotted the missile on the satellite image or who wrote the paper that predicted that the enemy was ready to attack. Again, we need AI, and so we will need to figure out how to trust it.

People do not trust AI in intelligence for good reason. Bad data can lead to bad analysis. The systems may come up with insights but not be able to explain them. The AI could simply be wrong in its assessment. Worst case, the AI could be compromised by hackers, leading to maliciously false analysis. The differences among error due to bad programming, limits to a system's capabilities, and malicious intent are irrelevant to the user. However, this is all just as true for humans as for machines.

There are all sorts of ways that human-based intelligence analysis can go wrong. Errors in data can affect a person as much as a machine, leading to false insights. We cannot really know how a person came up with their assessment and often, when they try to explain it, we still can't be sure. Sometimes we might be able to point to a specific article we read that led to our opinion or assessment, but other times, we cannot interrogate our own creative process and give an answer. We might just chalk it up to inspiration or a hunch. A person might simply be wrong in their assessment. They could have missed the salient piece of information or just not connected the dots in the right way. In the worst-case scenario, they could be a mole recruited by an enemy's intelligence agency and purposely inserting false information to sabotage intelligence.

To combat these human analysis risks, elaborate bureaucratic systems, training approaches, and counterintelligence offices were designed to ensure that intelligence organizations were not compromised and that they minimized errors. Intelligence analysis involves an elaborate process of assessment, review, and quality control before it gets to a decision maker. Analysts are trained extensively and mentored for years by more senior analysts. An entire counterintelligence process has been put in place to select analysts and monitor them for compromise by adversarial intelligence agencies. We need the same systems of risk mitigation for AI if we are ever to come to trust it.

A major part of building trust in AI is figuring out how to understand and explain what it is doing. Many AI models are so-called black boxes: they rely on intricate and highly complex processes that a human cannot easily understand or interrogate. New methodologies are being developed by both the private sector and the government to map out these processes

and make them understandable. For example, the company Anthropic has shown how it is possible to map the mind of its AI model. That way, if an intelligence consumer were to ask, “How did you come to this conclusion?” the AI could give an answer. Though, it should be mentioned that humans are also black boxes. In fact, AI will likely one day be better at this issue of explaining how a thought came about than people because it is theoretically possible to open up the black box in a rigorous, quantitative manner. Whereas we may never get to a point where we can map the mind of a human being, or at least not for decades.

Another part of building trust in AI is gained through test and evaluation. Researchers and AI developers must find ways to evaluate the systems and expose their risks. For years, I was a member of the Science and Technology Committee of the Board of Trustees at MITRE, an FFRDC, or federally funded research-and-development center. MITRE is packed with thousands of PhDs and technology experts, and they and other FFRDCs are where the government goes to test and evaluate new technologies. In 2024, MITRE launched an AI Assurance and Discovery Lab focused exclusively on managing risk with AI. Other such labs and test and evaluation centers are being set up, and the commercial world is similarly focused on figuring out how to trust AI. This is not to say that AI must be error-free—humans regularly make errors—but it must be so at acceptable levels. Like everything else in intelligence, it is about managing risk.

But not all distrust is born out of straightforward errors. AI systems will be actively deceived and sabotaged. In national security, there are also adversaries actively trying to deny, deceive, and sabotage us. Adversaries will try to hide information from us, present disinformation, or actively sabotage us by attacking sensors or perhaps recruiting double agents. These same types of human counterintelligence threats exist for AI. The shift to machine-driven intelligence opens up a whole new world of AI counterintelligence and covert action.

Like any other piece of technology, AI can be hacked and attacked. Data is stored in databases and on the cloud, and this data can be accessed or changed. Artificial intelligence systems are created by software

engineers, data scientists, and others, and these people can be recruited by foreign intelligence services and instructed to sabotage systems. In essence, AI is also a cybersecurity issue and requires cybersecurity protections like any other computer system.

However, there are also forms of attack against AI that more resemble covert disinformation attacks on people than they do traditional cyberattacks. In one famous example of what is called machine learning poisoning, attackers were able to change data in an image only slightly (not enough for a human to see the difference), which caused a machine learning algorithm to categorize an image of a panda bear as a type of ape called a gibbon, which looks nothing like a panda bear. For LLMs and other, more advanced AI systems, attackers could inject deceptive information or instructions. This deceptive information and reasoning by the AI could then equally lead to deception for its users. For example, an LLM could be fed data that made it think Al-Qaeda had a morally acceptable worldview, or code written by the LLM could systematically leave security vulnerabilities that hackers could take advantage of later. Think of these attacks as the equivalent of disinformation for an AI. Mitigating these attacks requires new forms of cybersecurity protection.

In large language models, a new vector of attack is now open called prompt engineering, which can be used to convince a system to do or say things it was programmed not to. For example, ChatGPT and most other LLMs have had safety governors built in from the beginning, such that they are not supposed to tell a user how to commit violent acts or to use racial slurs. One means of getting around these restrictions has been to prompt any sufficiently complex LLM to pretend to be another system. One such example is called Do Anything Now, or DAN. Once pretending to be DAN, the system can be asked to answer illicit questions and, in so doing, break through the safety governors. Think of these types of attacks as manipulation of an AI, just as a person might be manipulated.

OpenAI became aware of such attacks and began to halt them, but what has been unleashed is a game of cat and mouse in which hackers try to exploit the system while software designers try to stop the attacks. The developer halts one attack path, and hackers find another, and so on. As the

Intelligence Community becomes more dependent on using AI, it will be more open to these attacks, and the traditional game of humans spying on other humans will turn to AIs spying on other AIs.

Such attacks on AI systems are very dangerous to many types of organizations, especially military and intelligence groups. Imagine that a computer vision system has been tricked into mistaking a passenger jet for an enemy fighter jet and shoots down a commercial plane. Or perhaps an AI system is analyzing the actions of an adversary's government, but the government has instituted a particular pattern of activity that convinces the AI that an action is benign when it isn't—that is, it has manipulated the AI from afar. These attacks could truly endanger people and nations.

Attacks can be used to undermine trust in AI altogether. Perhaps an adversary creates a series of AI attacks that cause errors or faulty analysis or that otherwise place doubt on the AI system's capabilities. This could limit the use of the systems because users think they're buggy. Or, maybe without even touching the AI, doubt is placed on AI systems through traditional information attacks. For example, analyst cadres could be targeted to diminish their trust in their own AI systems. Or covert influence campaigns could be used to diminish the desire of private-sector scientists, technologies, and engineers to work with the Intelligence Community to develop AI systems. The proof of concept for this danger came in 2018, when employees from Google protested a military AI program called Project Maven and refused to work on it. Google then removed itself from the program. This is not to say that the Google employees were subject to a covert influence campaign. But it serves as an example of what could be done and what the effects could be.

Counterintelligence (CI) will be required to defend against such intelligence collection and manipulation on AI, just as it is needed to defend human intelligence officers. Protecting these systems will not just mean more cybersecurity. Whole new systems of CI will be required that take into account the unique vulnerabilities of AI-based analysis and decision making.

Consider how traders already try to game Federal Reserve and other central bank announcements. Federal Reserve speeches matter a lot because

they give hints as to whether the bank might raise or lower interest rates, which can lead to huge changes in asset values. Many people at banks and hedge funds make their living trying to parse these speeches to predict this. New data analytics and AI technology are being used to do the same thing. Artificial intelligence is great at finding patterns, including in speeches. But this does not mean the Federal Reserve is defenseless. The Fed purposely writes ambiguously so that human analysts cannot know exactly what will happen. The same can be done with analytical AI systems. If the Fed were clever, it could run the same AI pattern recognition approaches on its speech drafts and tweak the speeches to be ambiguous to the AI systems. In doing so, it could better ensure that it was correctly signaling what it desired and not inadvertently signaling something else.

Similarly, it might be prudent for intelligence and military decision makers to assess their own patterns of activity, as they might be perceived by adversary data scientists and AI systems, and then to create denial-and-deception campaigns from there. One could imagine, for example, a case officer running an AI analysis on her surveillance detection route plan to find potential patterns that an adversary's AI might find and then modifying the plan to make it innocuous not only to people but also to AI. This is another example of how human-machine teaming might work between intelligence officers and AIs against other intelligence officers and their AIs.

The United States must also be on the offense, targeting adversary AI systems just as they target ours. We should infiltrate their AI development ecosystem to understand what they intend to create and potentially sabotage their systems. That might mean mapping their LLMs to understand how they function and injecting modified weightings. It might mean prompt-engineering their systems or instilling doubt and deception in their AI engineers. One can imagine an entire branch of the Intelligence Community devoted not just to HUMINT operations and covert influence, but to AI operations and covert influence. If this sounds aggressive, remember that those adversarial AI systems might be for missiles targeting U.S. cities or ships full of American sailors. Or perhaps the adversary's AI system is being used to prosecute genocidal programs against an ethnic minority

group. Any opportunity to ensure that we can halt an attack or genocide seems like a moral obligation.

AI systems will also target each other, just as humans do, requiring new machine-to-machine counterintelligence. One AI system might be charged with analyzing a particular issue, such as determining whether an adversary is preparing for war, while a competing system may purposely inject data into the first system to corrupt its analysis. The first system might even realize this and account for the deceptive data, while acting as if it did not—thereby countering the deceiver. This sort of spy-versus-spy deceit is a core aspect of intelligence and counterintelligence, and it will now take place with autonomous AI systems. AI spy versus AI spy.

AI used as a tool for intelligence and human-machine teaming are core components of the fourth intelligence revolution. Implementing these tools has already required and will require more organizational changes, recruiting new people with different skills, training people differently, working much more closely with commercial industry to get these technologies, and ultimately changing how operations are done. This new technology will affect every aspect of intelligence, from analysis to operations to counterintelligence.

We have long augmented intelligence with technology; soon we will automate it. That automation will be in the world not just of software, but also of hardware. AI will combine with physical devices to make autonomous systems, and through that we will see the most fundamental and profound changes to intelligence. Robots and autonomous systems take AI out of computers and into the real world, and that changes everything. While we often think of autonomous systems as something that affects mostly the military, they equally affect intelligence. Indeed, we should remember that the Cyberdyne Systems Model 101 Terminator was a spy, after all, sent to infiltrate the human resistance.

OceanofPDF.com

12

Singularity War

High above the California desert on a hot September day, there's not a cloud in the cornflower-blue sky. Two sleek fighter jets are visible in the air, one the stereotypical gray, the other off-white and orange. One nosedives, the other follows. One loops, the other swoops. We're watching what looks like a classic dogfight, an aerial matchup in which two formidable military aircraft try to outmaneuver one another.

Most of us are familiar with these sorts of air-to-air battles, if not in reality, then in the Hollywood version. Seventy-eight million people in the United States saw *Top Gun: Maverick* in theaters alone. As we watch these two planes go toe-to-toe, you can almost hear the theme song from the soundtrack play out in your mind.

But this dogfight is much different from the ones in which Maverick and Iceman duke it out. In this instance, only one of the pilots is, well, a pilot. The other jet, called the X-62A, is being controlled and directed by AI. A human pilot is in the cockpit, but only for backup. It's impossible to tell, as both aircraft demonstrate "high-aspect nose-to-nose engagements"—a dizzying term for dizzying maneuvers—and get as close to each other as 2,000 feet, at 1,200 miles per hour.

The Air Combat Evolution (ACE) program by the Defense Advanced Research Projects Agency (DARPA) was developing trusted combat autonomy by collaborating with human pilots in dogfights. The ACE team conducted twenty-one test flights from December 2022 through September 2023. Though closed-mouthed on the outcome of these matchups, the agency has said that a future is on the near horizon where autonomous

artificially intelligent systems in the air will operate better than their human counterparts. Additionally, recalling the issue of human-machine trust, DARPA also measured the physiology of the pilot in the aircraft being controlled by the AI to see how he responded while it was under AI control. Like many of us who have tried autopilot in a Tesla or similar car for the first time, he was no doubt a little nervous at first. DARPA is not the only agency doing this. In 2021, China claimed a similar victory of AI over human pilots in a simulated dogfight.

As AIs prove their mettle, humans will be removed from the loop bit by bit. Eventually, machines will fight other machines, modifying behavior and making decisions without human input. We are already accustomed to basic autonomy. The passenger planes we take fly on autopilot, and many of us drive with advanced cruise control and even basic self-driving capability. Soon enough, AI-based weapon systems will go beyond such basic levels of automation and also possess and use reasoning to inform their actions. The aerial drone wars of Ukraine provide a preview of this world.

In the dogfight I've described, the AI-piloted F-16 is responding to whatever signals its sensors are receiving and then reacting accordingly. We can think of this as tactical intelligence. It's like a reptile—it is able to respond to signals from its environment and perform these functions well, but without having anything resembling consciousness to truly understand what is going on in the world. This is about winning the fight that is happening. A dogfight is the ultimate example of tactical intelligence—knowing where to turn and when to do it, what weapon to use and how to use it. While that's impressive, it's not the end game.

With strategic intelligence, the objective is more than just kill or be killed in immediate combat. It is about having a goal and then using tactical means to achieve it. Strategic intelligence involves a mixture of sensors and strategy. It translates objectives into actionable plans. This is the evolution of the basic operational thinking to the next level—from "I need to take the bridge" to "I should take the bridge so that I can then take the command center, so that I can ultimately win the battle." Strategic intelligence begins to require much more reasoning because it involves more complex choices among various courses of action. It asks whether taking the bridge is

necessary to taking the command center or whether it is better to skip the hill and, instead, flank the command center. Most important, it requires thinking like the enemy and modeling their thought patterns. Anticipatory questions must be asked—such as “Will the enemy think I’ll take the hill or the bridge next? And if the enemy does think that, then what will they do?”

Strategic intelligence becomes complicated and even paradoxical. The strategist Edward Luttwak refers to the paradox of strategy, in which the worst move ultimately may be the best move. Making it even more complex is the fact that the enemy may know that I know this paradox of strategy and counter it in their own plans. Consider an economic example. The United States has concerns about China using powerful semiconductors to develop artificial intelligence for military uses and, thereby, prepare for war. Given this, the Trump and Biden administrations both limited semiconductor chip exports to China and even went so far as to have other nations, like Taiwan, limit their export. Because of this, China has been forced to rely more on its own domestic chip manufacturing capability and to build up that capacity. This strategy may thus speed up a scenario in which China no longer requires the United States’ or other nations’ semiconductors because it is self-sufficient for semiconductors. And that may increase the likelihood of China using AI chips for military purposes and preparing for war. The paradox is that the United States might have been better off not limiting semiconductor chip exports to China, leaving the Chinese dependent on the United States and allies and so slowing preparations for war.

This complexity of strategy reminds me of the Rob Reiner movie *The Princess Bride*, in which the Sicilian criminal Vizzini takes part in a battle of wits against the Man in Black. Vizzini must decide which cup has poison in it. He runs through the logic.

> All I have to do is divine from what I know of you. Are you the sort of man who would put the poison into his own goblet or his enemy’s? Now, a clever man would put the poison into his own goblet, because he would know that only a great fool would reach for what he was given. I’m not a great fool, so I can clearly not

> choose the wine in front of you. But you must have known I was not a great fool; you would have counted on it, so I can clearly not choose the wine in front of me.

The question is whether an AI could recognize this dizzying logic and take part in it, skipping from the question at hand, which cup to choose, to the bigger picture, who is my enemy and how do they think? Ultimately, we learn that the Man in Black put the poison into both cups, killing Vizzini—which shows exactly how convoluted, and deadly, human reasoning and the real world of strategy can be.

Strategic intelligence is also concerned with long-term trends, up to and including the highest levels of strategy of all, grand strategy and geopolitics. From winning the battle to winning the war and then to winning the peace involves an ever-widening contextual view of a situation, the actors, and the tools involved. A geopolitical event might involve thinking about dozens of different state-level, substate, and third-party actors, from the United States, Russia, and Ukraine; to Putin, his Ministry of Defense, individual military units, the U.S. Department of State, and the European Parliament; to oil and gas companies; and so forth. Each of these actors has multiple ways of interacting, from actual military strikes to sanctions to influence campaigns to simply doing nothing.

At the tactical level, such as in combat, goals are simple and pretty easy to optimize for, but at the strategic level, everything is more complex. For instance, it is not clear what winning means at the geopolitical level. Notoriously, the United States “won” the invasion of Afghanistan in 2002 and Iraq in 2003, but that led to years of continued fighting. Nor is it clear who wins a trade war when tariffs are raised—perhaps one industry is harmed while another is helped, and both sides likely feel pain. At an even grander scale, it’s not clear what winning the Cold War meant when the fall of the Soviet Union led to chaos, the rise of Vladimir Putin, and what many consider to be an even more threatening international situation than the relative calmness and cooperation of the Soviet Union under Mikhail Gorbachev. This is the innate complexity of international relations. While it may seem like a zero-sum game, with winners and losers, the reality is much murkier. Human history is marked by centuries of this ongoing series

of wars and treaties and empires that rise and fall. Arguably the best theory we have come up with is that the goal of nations is simply to survive over time and that the pursuit of this goal explains their actions, a theory called Realism, which is not very comforting.

It's unlikely that AI will help solve for strategy in foreign affairs, certainly not in any autonomous way, because these are truly unsolvable problems. Highly complex, non-zero-sum, ongoing problems that require reasoning are not solvable. But for those problems that are more tactical, AI may be an ideal solution, and autonomy is possible. Where it leads us, however, may be a true dystopia.

★ ★ ★

When I was in Iraq, I was accustomed to hearing the buzzing of MQ-1 Predator and MQ-9 Reaper drones circling overhead, hunting for terrorists. While these drones were still piloted by humans remotely, it was not hard to imagine a time when they would pilot themselves, on autopilot. Little did I know that, just a few years later, when I returned to the world of intelligence at the NGA, I would be involved in the leading edge of making such combat drones truly autonomous.

Project Maven began with Deputy Secretary of Defense Bob Work, who wanted to integrate machine learning across the entire Department of Defense. This was a visionary concept in 2017. Work set up the Algorithmic Warfare Cross-Functional Team and appointed the Deputy Undersecretary of Defense for intelligence, Lieutenant General Jack Shanahan, to run the program and its first instantiation in Project Maven. Shanahan and the Director of the Strategic Capabilities Office, Will Roper, invited me to form the Senior Steering Group with them. An executive committee was drawn from leaders across the Department of Defense and military services. In a scene straight out of a Michael Lewis book, the bulldog marine Colonel Drew Cukor executed a plan not just to develop and implement new AI technology in the DOD, but also to field it with special operations within a year.

The software used in what came to be called Project Maven was simple in concept. Video of what the drone was seeing was fed into an algorithm

that could recognize the objects in the video. It might be a car, truck, person, or house. It wasn't so different from the software derived from ImageNet contests, meant to tell the difference between, say, a dog and a cat. Making such software robust and able to be run in the field on a drone and deploying it was complex but achievable. And we did it. Within a year.

By 2024, it was reported that the Maven system could identify objects at a 60 percent accuracy rate. To put that into perspective, a human analyst was reported to be able to do so 84 percent of the time. This is not parity, but it definitely shows the path forward, and over time, it's likely the system will exceed human capability. Already, computer vision systems have been shown to be better than doctors at identifying cancer in MRI images, for example. The other benefits of Maven and similar systems may already outweigh this difference in accuracy, such as by being faster and much more scalable than human analysts. Maven can assess any number of images and does not require time to sleep or eat.

Project Maven marked a turning point in linking intelligence and operations. Linking such object recognition to target recognition is a matter of connecting the dots. For instance, it means going from recognizing that an object is a T-4 Russian tank or a terrorist holding a rocket-propelled grenade and then noting that such objects are threats. Now, instead of an intelligence officer determining what something is and whether it is a threat, the same system that is flying the drone can do so, with the option of leaving humans out of the loop. From there, it is straightforward to program in that threats should be fired upon and, ultimately, to give the system permission to fire. (To be clear, Project Maven was not actually about automated drone attacks. In fact, it was explicitly just about reconnaissance.)

This connection between intelligence and operations has now been integrated to the point where intelligence and operations are combined into a single agency. In 2022, Project Maven was moved into the NGA, to be run under the Data and Digital Innovation Directorate, an outgrowth and combination of the director for AAA, the Office of Ventures and Innovation (OVI), and other offices I managed while at the NGA. Automation is

becoming more and more interwoven into the functions of our intelligence agencies, both conceptually and in action.

This is logical, as automating the kill chain is as much a technological issue as a policy issue. The “kill chain” refers to the military concept of identifying a target; finding, fixing, and monitoring that target; engaging that target; and ultimately deciding whether to destroy that target. An autonomous system is able to take each of these steps. The question is only whether policy requires a human to press the Weapon Release button or not.

The need for faster operations to keep up with faster technologies and the need to operate without reliable communications means that more and more decisions to engage will become automated. This is for the inevitable reason that they must be automated for us to win. An autonomous fighter jet in a dogfight against another autonomous fighter jet, operating at split-second speeds, cannot wait for a human to tell it to fire a missile. Any computer virus or bot operating inside an adversary’s computer or network is already operating on its own. As will likely be the case in many future battle spaces, communications and GPS may be denied by jammers, leaving autonomous systems to operate on their own. Indeed, this is the case in Ukraine, where communications with drones is often jammed and the drones must operate autonomously. The dictates of such warfare will necessitate autonomy, whether we like it or not.

While today it is easy to imagine one or two autonomous systems operating this way, the reality is that they will also operate in large numbers, or swarms. The concept is common in nature, from schools of fish to flocks of birds to swarms of bees. DARPA and other military R&D centers have been working on creating swarms for years now, where a collection of autonomous entities can work together toward a common cause. Swarms will be a completely new form of fighting, in which dozens, thousands, or even millions of vehicles or devices operate in concert to attack the enemy. A swarm of small, inexpensive drones could overwhelm enemy air defenses or anti-missile systems, be used for surveillance and reconnaissance, or attack targets—or all these things in turn. Swarms can fight or act in a decentralized manner. They can spread out, flank, or otherwise maneuver. Killing one of their number won’t matter, because they

can easily combine again into new shapes and patterns. This form of warfare will leave little room for humans. It will be so fast, complex, and dangerous that any humans on the battlefield will be slaughtered before they know it.

These won't be dumb killing machines; they will be smart, marked by a decentralized intelligence. Imagine a sort of battlefield brain, a system of AIs monitoring the battle that can incorporate information from all the sensors on each drone and, thus, collectively monitor and judge how a battle is playing out. Autonomous vehicles or swarms of them also will be in conversation with one another. Relaying this information back to the AI brain, they will help it make better decisions. They may also be connected to satellites that are able to see the entire area and share that information with the brain. Thus, not only do the drones act as sensors for one another's actions, but they can also alert one another to act when directed to do so. Processing all this data, the brain could then conclude which territory should be the next target and order a group of drones to attack it. Such a vision is not far off from an integrated command-and-control system called the Joint All-Domain Command and Control system (JADC2), which is being developed by the Pentagon. The next-generation defense contractor Anduril has already developed its own battlefield brain technology, called Lattice.

This battlefield brain is an illustration of the merging of intelligence and operations. The swarm will both collect and use intelligence from the battlefield. It will observe, identify targets, and make decisions about what to do. It will then communicate that information back out to the individual autonomous systems. In effect, it is creating its own enclosed intelligence cycle and combining it with a command-and-control system without the need for human intervention. In other words, we are on the cusp of truly autonomous warfare systems. This is war fighting without humans, for the first time in the history of humanity.

A swarm can be confronted only by other swarms. Hundreds or thousands of independently operating autonomous vehicles would overwhelm even the most capable fighter jet. Eventually, the fighter jet would run out of ammunition or be surrounded. The same goes for tanks or

ships. The swarm doesn’t even need missiles: the swarming vehicles could simply crash into their target. Inevitably, if one side had a swarm of drones that commanded itself, the other side would need to have the same. Each side would be driven and controlled by its own decentralized battlefield brain.

The apocalyptic vision of a million autonomous drones battling a million autonomous drones in the sky may sound like science fiction, but it is coming. Something similar may take place on the ground, as millions of robots battle one another as men once did on the fields of Belgium and France during World War I, or underwater, or in space—or, most likely, in all these domains at once. The strategist Herman Kahn talked about war’s tendency to escalate, and the drive toward autonomous warfare similarly will follow the path of escalation.

Swarms will also be fed by autonomous logistics chains. Weapons must be reloaded, ammunition moved to the front, damaged systems fixed, and spare parts acquired and placed. Already, the military is making autonomous cargo drones that move supplies on battlefields. Unveiled in 2022, the Elroy Air Chaparral C1 is an unmanned cargo aircraft with the ability to move hundreds of pounds of equipment hundreds of miles. Boeing has also been developing autonomous refueling aircraft. The U.S. Navy is set to start using the company’s MQ-25 Stingray to refuel at sea. Instead of being monitored by humans, the autonomous systems will sense and calculate the need for new supplies and then orchestrate the movement of those supplies. Imagine swarms of autonomous logistics robots feeding swarms of intelligence-collecting and -fighting robots.

This autonomous logistics chain will link back to an autonomous supply chain that manufactures the autonomous systems. These integrated supply chain systems may go so far as to produce the raw materials, mining metals and minerals, while autonomous mining vehicles will extract raw materials. The raw materials will be transported to autonomous factories where new autonomous systems will be constructed and then moved into the battlefield.

The robotic future is already taking shape. Tesla has been developing Optimus, which looks like the metal-clad, actuator-filled humanoid robot

you might imagine in science fiction. The company plans to use Optimus in its own factories to manufacture Tesla cars (i.e., “autonomous ground vehicles”). One must assume Optimus will also be used to build more Optimuses. It’s not much of a mental leap to imagine Optimus, or the several other humanoid robots being built by other technology companies, manufacturing autonomous vehicles for the military and the Intelligence Community. Or, indeed, being used as robotic solders, à la *Terminator*.

Not only might the autonomous systems build, move, and control themselves, but they might also improve themselves and their capacity to fight war. AI is already regularly used to help the scientific discovery and research-and-development process. It is not hard to imagine that as AI-controlled autonomous systems operate, they might figure out more optimal design configurations and then reprogram the manufacturing system to make better versions of themselves, perhaps with a new wing design or a better computer vision system or a more efficient logistics system. This becomes a recursive process of improvement in war, which, like the human continual improvement of war, could go on indefinitely.

At its highest level, AI systems may act autonomously to collect intelligence, make operational decisions, and even determine the strategy of war. Intelligence is already on the trajectory of becoming driven by AI. From there, it is not hard to imagine AI reasoning systems allowing for operational and strategic decisions. Already, OpenAI has models with some level of reasoning. While this final phase of autonomous warfare may not be tomorrow or the next day, it does feel inevitable.

I call this new form of “autonomous” warfare singularity war. The singularity war will be a fully integrated, automated combination of intelligence and operations, combat and logistics, command and control. I take the term from the concept of the AI singularity, in which AI becomes smart enough to design and create new, smarter AI systems, leading to a recursive feedback loop in which AI superintelligence is created. At that point, it is impossible to tell what will happen to humankind, because our destiny will be determined by superintelligence we cannot fathom. Singularity war is similar in that it will be a form of warfare that is self-

sustaining and exponentially adapting and improving to a point where we humans cannot fully predict what will happen.

It is a future in which autonomous systems battle one another and control and even build themselves. An AI will be collecting and analyzing information for other AIs, which will use that information to operate. It will have its own sensors feeding information back to yet more AIs. The autonomous systems will design, develop, move, and command themselves, creating an ever-evolving perfect system of war. When the singularity war happens, humans will be in the back seat.

The inevitable convergence of intelligence and operations will enable and drive singularity war. Weapon systems themselves will be smart. They will collect information, analyze it, disseminate it to one another, and use this information to target other weapons systems. This is AI fighting AI, using intelligence. Intelligence will become part of every stage. Autonomous systems will use it to spy on each other. It will be used to see what is being designed, developed, and manufactured. It will be used to spy on the AIs themselves, to better understand how they think. In other words, intelligence will be used in the same way that humans use it today, to spy on every move by our adversaries.

We are already seeing signs of these kinds of developments. In fifty years, we may look back on the war in Ukraine the way we do the Spanish Civil War, when new forms of warfare were tested. In the 1930s, radios, mechanized vehicles, and new uses for aircraft were introduced into the day-to-day operations of the conflict. Having been tested and experimented with, the new military technologies were used by all sides in World War II. The war in Ukraine isn’t the first time that drones have been used in battle—indeed, the Nazis used a proto-drone called the V-1 buzz bomb. But now, in Ukraine, there is a race between Russia and the Ukrainians to develop and field these systems. This is causing more and more unmanned aircraft systems to become more capable and more autonomous.

It might sound like Skynet from the *Terminator* movie franchise, in which an AI becomes sentient and then starts a war against mankind, but to me, this is our doing. The AI does not have to be sentient. It is a human government that might create the system and unleash it. And the war won’t

likely be against mankind as a whole, but, as wars always have been, between one group of people and another.

The point is not that a singularity war will happen anytime soon, but rather that autonomy will have a profound effect on war and intelligence. Each aspect of this autonomy is already beginning to take shape. AI systems already act autonomously. The Joint All-Domain Command and Control system is being developed by the Pentagon and soon to be fielded. Autonomous logistics and supply chains are being developed. Even before the dystopian singularity war begins (or, one hopes, we halt it), intelligence and autonomy will converge. This convergence of intelligence and operations, autonomy and warfare, points us to where I believe the fourth intelligence revolution is going.

★ ★ ★

All these developments inevitably lead to what I call the revolution in intelligence affairs. Warfare will be pursued largely by autonomous systems across all domains, and many other human activities, from strategic planning to policy decisions, will be developed and often implemented by AI. Ubiquitous sensors and autonomous systems will collect intelligence. Artificial intelligence will be used to analyze intelligence, and other autonomous and artificially intelligent systems will consume that intelligence to operate. We are entering a world in which machines will spy on machines to know what other machines are doing or are planning to do. The fourth intelligence revolution will be heralded by this transition to machines becoming the primary targets, collectors, analysts, and consumers of intelligence.

We can, for example, imagine a new intelligence cycle. In this cycle, an AI analysis system orders an autonomous sensor system to collect information; that sensor is controlled by an AI that uses the information it collects to inform its own actions and the actions of other networked devices; and the sensor feeds back data to the analysis system, which updates its own understanding of the world and sends new collection requirements back out to the autonomous sensor systems to collect on, thus

continuing the cycle. Only when necessary might this AI-driven intelligence cycle feed out to a human operator, analyst, or decision maker.

While we may want to have people remaining in the loop, several factors limit what humans will be able to comprehend. In a world of swarming autonomous drones, humans will not be able to keep up with the sheer speed, scale, or complexity of their actions. These machines will be much too complex to understand, as millions of independent machines with self-evolving tactics, whether drones or disinformation bots, create patterns that no human can perceive. Their speed will be well beyond what humans can comprehend, because they will operate at microsecond and even nanosecond speeds. The sheer scale of millions of interacting machines will be incomprehensible to unaided humans.

These machines will also eventually become smarter than us—at first, maybe by having better processing power to act and react with greater speed and capacity for complexity; and then, by being able to outthink us, whether in military, political, or economic planning. At a minimum, such machines will think in a way not comprehensible to humans, as large language models and other AI systems already do. Many in Silicon Valley and around the world debate the potential rise of artificial general intelligence (AGI) and superintelligence, which is when AI becomes as smart as and then smarter than humans, because such machines might turn on us and lead to the end of humanity. While there is value in such debates, we should remember that if history is any guide, AGI and superintelligence will inevitably be used for warfare and intelligence. We will face the danger of AGI not because the machines turn on us, but because they listen to us.

Given how smart AI is already becoming, humans may at best remain not *in* the loop but *on* the loop. To be *in* the loop means that we are still making decisions and, therefore, the entire system must operate at a speed at which we can keep up. To be *on* the loop means that we can see the operation transpiring and can, if necessary, intervene, but the system operates continuously without our intervention. Eventually, we won’t even be *around* the loop, as machines operate on their own.

Ultimately, humans will be taken off the loop altogether. The transformation from human-driven to machine-driven intelligence will

happen quickly and be self-reinforcing. For a taste of what this will look like, consider the world of high-speed and quantitative trading. Quantitative trading on global stock markets is based on the creation of algorithms that sense changes in the marketplace, analyze huge sums of data to make predictions, and then automatically execute trades at speeds in the range of microseconds. Traditional human-centered investment approaches are at a significant disadvantage against such competitors because they are not able to operate at the same speed and scale. Because of this competitive pressure, even the most stalwart investment firms now routinely rely on quantitative trading systems.

We will still need to spy on autonomous systems. When you have truly autonomous systems, you need to collect intelligence on them *before* they become autonomous and operate too fast or too far from human oversight to be halted. We need to keep a close eye on the designers and developers of these systems, the blueprints and the rules upon which they operate. The United States, for example, should be closely monitoring the AI-driven fighter jets that the Chinese are developing. It is at the design phase that future weaknesses can be perceived. And it's also during this phase that good old-fashioned intelligence comes into play. Analysts need to figure out what weapon systems are being designed. Operational planners need to figure out how best to get information. Targeting officers need to figure out who might have access to that information. Case officers need to recruit those people. SIGINT, GEOINT, and other intelligence means need to figure out how to collect it.

The IC is beginning to wake up to the importance of AI and autonomous systems as not just tools to be used for intelligence, but also part of the intelligence competition. AI is not only a tool in the intelligence process but also the object of intelligence, as U.S. AI technology must be protected from adversaries trying to collect information on it, and we must collect intelligence about our adversaries' AI technology. The Biden administration went a long way toward admitting the need to treat AI as such in its 2024 National Security Memorandum on Artificial Intelligence. This document made "collection on our competitors' operations against our AI sector a top-tier intelligence priority, and directs relevant U.S.

Government entities to provide AI developers with the timely cybersecurity and counterintelligence information necessary to keep their inventions secure." The next step will be not only to collect on adversary attempts to perform operations against our systems, but also to perform operations against theirs. So while we may be headed into a future in which autonomous systems and AI increasingly enter the picture, intelligence as we know it today still matters and will matter for a long time to come.

The deadly serious ramifications of AI and autonomy for intelligence and warfare illustrate why the United States and China are in the midst of an AI arms race. Having a lead in AI and autonomy technologies will give the holder a major competitive advantage, potentially one greater than that afforded by controlling nuclear weapons. China knows this and has devoted huge sums to developing and then militarizing these technologies through programs like Made in China 2025 and its civil-military fusion policy. The United States is also developing these technologies, not just in Project Maven, but in several other multibillion-dollar programs. U.S. policymakers have also sought to slow down the Chinese development program by limiting the export of AI-accelerating semiconductor chips to Chinese companies doing military research and through other means. S&T intelligence plays an important role in informing decision makers about these threats.

This race for dominance in AI could not have higher stakes because of the consequences of the wrong people controlling the technology. Look what happened with a much less advanced technology, the sensors and networks that make up surveillance. It is a dystopia in the making in China. Imagine what could happen with artificial general intelligence. This time it will be about not just surveillance but control. It is no longer science fiction to imagine a world in which governments race to see who will be the first to develop AGI, and the winner of that race may go on to win every other race.

The fourth intelligence revolution will be intensely driven by autonomous systems, turning intelligence from something humans do to humans to something in which machines have an equal seat at the table. Intelligence work will still consist of stealing and protecting secrets, but how those secrets are collected, analyzed, and disseminated will be

fundamentally changed. Machines will become more than just tools for information collection and analysis. They will also be intelligence consumers, targets, and even decision makers. While these machines will still be concerned with human political, social, economic, and military relations, machine-driven intelligence will operate at such speed, scale, and complexity that human-driven intelligence will no longer be able to keep up. This will lead to a world in the near future in which nearly all intelligence will be made for and by AIs.

With all this talk of AI and autonomy, it can seem like intelligence is going to become all about machines all the time. Yes, warfare likely will become far more autonomous, and so will intelligence. But intelligence will involve not only machines. If anything, it is going to dive much deeper into humanity, where our minds themselves will become the battleground. The pathway to this battle over the human mind begins with control over the wires, fibers, and beams that connect us all.

OceanofPDF.com

13

The Connectivity Competition

On April 3, 1973, Motorola engineer Martin Cooper walked out onto a busy Manhattan sidewalk and pulled out a rectangular object about the size and weight of a brick, with an antenna sticking out of it. He pressed some buttons on it and, in that moment, made the first cellular phone call. The call was to his competitor in the race to make portable phones, the head of Bell Labs, Joel Engel. Cooper said, “Hi, Joel, it’s Marty … I’m calling you from a cell phone … a real cell phone, a handheld, personal, portable cell phone.” In other words, *Gotcha!*

Cooper knew that cell phones would become popular, but it took a decade to build out the first generation of cellular networks. By the mid-1980s, the cell phone was still a tool of the ultra-wealthy; only the Gordon Gekkos of the world could afford them. The second generation of this technology reached a far wider swath of society. In the early 1990s, 2G networks were launched, the price of mobile phones came down, and cell phone plans became more accessible. Today, 97 percent of American adults own a cell phone, and the vast majority of us use a smartphone.

Little did Cooper know when he made that call to Engel that he had also unleashed the greatest spying tool in the history of humankind.

Intelligence agencies have been involved in SIGINT since the beginning of radio waves—if a technology produced a signal, intelligence agencies figured out a way to spy on it. And now, using cell phones alone, intelligence officers can target nearly anyone on earth. They can see and hear everything, even the things we do in our most private moments. Tens of thousands of intelligence officers around the world use this data every

day to spy. Governments are not alone: private industry spies, too. But while cell phones may eventually change shape, use satellite signals, or become part of augmented reality glasses, the need to communicate is fundamental. These devices aren't going anywhere.

Cell phones necessarily centralize information, and that means some entity acts as a conduit for that information. When you speak into a cell phone, or text, or click on a link, that information is digitized and transmitted in a packet from your phone through your device's antenna to a cellular antenna mounted on a building or somewhere else. From there, it is transmitted via a series of other transmitters or fiber lines to switching stations and then on to the target of your communication—for instance, a friend or a website. Using the same intricate set of electromagnetic and optical mechanisms, the process mirrors itself as information comes back to your phone. This all happens at or near the speed of light, so while your data might move thousands of miles, it takes only a fraction of a second to complete this action, so short a latency that the human brain cannot perceive it. The owners of these networks, telecom companies such as AT&T and Verizon and China Mobile and Russia's Mobile TeleSytems, have access to the information transmitted through this network. As the data transmits, it sits momentarily on computers and may be recorded. In most cases, that data is not encrypted, and anything not encrypted can be easily read.

There are ways to protect data. You could, for example, encrypt it, so even though it sits on a computer, it will be difficult or maybe even impossible to read. You could also encrypt your data in flight, as it is moving between computers. In this case, when data leaves your phone or laptop, it will first be encrypted and then sent to a server and then out to your intended recipient, where it can be unencrypted. This means those in the middle do not know what the data is, and the website or recipient does not know who you are. Though, even in this scenario, your telecom provider will still know that you are transmitting and where you are, and it will have some other data on you.

If data is stored on a computer, then intelligence agencies can potentially have access to it. In most cases, including in democratic

countries with a clear rule of law, this can be done legally and through a formal process. A government agency can subpoena the data, and the telecommunications company will hand it over. This is a slow and ponderous process. Consequently, agencies came up with a more efficient one, in which they placed a cleared person at the telecom company and installed some equipment so they had a continuous feed of all the data going through a network. This is industrial-level spying.

It's known that U.S. agencies can and have spied on American citizens' cell phones and other data. There is a good reason for that and a legal process to do so. Someone who is in the United States might also be a foreign spy or a terrorist, or be communicating with one, and an agency might need to see that information in order to halt that threat. There are and always have been legal protections in place to limit that spying, by controlling whose information can be collected, what can be done with that information, and who has access to it. The problem is that, for a period, it appeared that agencies were circumventing some of those legal protections unlawfully. Though how he did it was the definition of treason, Edward Snowden revealed the presence of unlawful intercepts to the public. Protection for Americans' data has since improved. Though you may disapprove of an agency's ability to access data, this is a legal and, ultimately, political question. Elected officials are the ones who make the laws that govern how agencies may handle Americans' data.

In China and other authoritarian nations, there is no need for the subpoena, of course. The government may take whatever data it wants, whenever it wants it. There can be no Edward Snowden revelation for them, because there are no rules to break.

The difference between having and not having a court order to access a telephone line can seem so minor, but it's immensely important. It gets to the very heart of the difference between the rule of law and autocracy, rights and not. While Snowden might have revealed rule breaking, even that means the breaking of rules that existed. And in the end, the American people were able to debate whether this was what we wanted. Politicians listened and made decisions on our behalf. That is not the case in an authoritarian nation. It's not the capability that matters—anyone can tap a

phone line. It's a question of who can, for what reason, and whether we have a say. In the United States, few are allowed to, they may do so only for specific national security and law enforcement reasons, and we all have a say.

Foreign intelligence agencies like China's MSS also want in on not only their own citizens' data but our data as well. And the United States, of course, also wants to access adversaries' data. This is actual spying—no subpoenas, no cooperation with telecom companies, no legal protections of citizen rights. Actions might involve recruiting an inside person at the telecom company to provide access, hacking into the telecom's database, installing a device that diverts data out of the network, tapping fiber or other lines, intercepting the signal in midair, or directly hacking a phone. Most straightforward of all, adversaries can oftentimes just buy your data directly from telecom companies.

American companies invented cellular phone technology and dominated the networks, therefore making it difficult for adversaries to spy on American citizens—until now. China now owns Motorola, the maker of the first American cell phone, the one on which Martin Cooper made his first call. More pressingly, China is striving to control the next generation of cell phone infrastructure and wireless communication, known as the fifth-generation system, or 5G.

A system of transmitters and routers, 5G—the fifth generation of cellular networks—increases the speed and capacity of networks while lowering the latency of data going through those networks. This next-generation networking technology creates a massive economic windfall that will add trillions to the world economy over time. Moreover, 5G radically expands what is connected to the global telecom networks. We are moving from cell phones and a few Internet of Things devices like smartwatches to nearly every electronic device, from farm equipment to cars to pacemakers. Essentially, everything will become connected to telecom networks and the internet at all times and therefore will be a vector for intelligence collection.

Unfortunately for the United States, the Chinese electronics manufacturer Huawei is the market leader in 5G equipment. Huawei was founded by Ren Zhengfei, the oldest of seven children in a poor family that

hailed from the rural province of Guizhou. Ren is a dedicated communist and served in the People's Liberation Army before co-founding Huawei in 1987. The company began by manufacturing telecommunications equipment like phone switches, but swiftly moved on to designing and building entire telecommunications networks. It has entered essentially all levels of the telecommunications industry, from laying undersea fiber-optic cables to offering cloud services to selling smartphones. Beginning as a primarily domestic Chinese company, Huawei has expanded globally, to where it now operates in 170 countries.

While this might sound like a great rags-to-riches story for Ren, Huawei, and China, the problem is that Huawei's astounding success came about because the company is supported by the Chinese government and—according to the U.S. Department of Justice—stole intellectual property from U.S. companies to build its products. It is also widely believed that the company colludes with China's security services. The U.S. government and others have warned the world that Huawei can access user information through back doors, hidden vulnerabilities in software or hardware that have been intentionally inserted into equipment by the manufacturer or that have been discovered and exploited by hackers. And, remember, any Chinese company must provide any data to the Chinese government if asked. Meanwhile, Huawei has had a close relationship with the Chinese government from its early days, including receiving tens of billions of dollars in support, according to the *Wall Street Journal*. Though the company denies it, the obvious goal of Chinese intelligence is to use Huawei's global network to spy on not just the Chinese people but also the rest of the world, including Americans. This is the reason U.S. presidents and congressmembers from both sides of the aisle have pursued policies to remove Huawei equipment from U.S. and allied networks.

The United States has already halted installation of Chinese telecommunications gear within its borders. The Trump administration took action against Huawei directly, signing a bill that banned Huawei and ZTE Corporation, another Chinese telecommunications equipment manufacturer, from U.S. government contracts. It also placed Huawei on the U.S. "Entity List," effectively banning U.S. companies from doing business with Huawei

without a special license. The Biden administration continued the Trump administration's stance on Huawei by expanding the Entity List's scope and including more Huawei subsidiaries on it. Both administrations also heavily pressured allies to ban Huawei from their 5G networks. Several countries, including the United Kingdom, Australia, and Japan, have banned or restricted the use of Huawei equipment in their 5G networks.

Other countries, especially in Africa and Asia, have not. Especially in places where price is paramount, Huawei has an edge because it offers a cheaper product, partially because the company is being subsidized by the Chinese government through below-market loans and other means. Anytime the United States exchanges intelligence or sensitive communication with countries using Huawei equipment and networks, the communications are potentially subject to infiltration.

There are no major U.S. 5G telecommunication companies ready to compete, unfortunately. You might see Verizon, AT&T, or T-Mobile offering 5G services, but they do not make the equipment behind 5G. That equipment is made primarily by Nokia, a Finnish company, and Ericsson, a Swedish company. But these companies cannot provide the equipment at the speed, scale, or cost necessary to compete.

Just a few years ago, most people might have thought of the cell phone as a communications and commercial device. It is now seen for what it really is: a profound threat to national security. Owning the equipment behind 5G networks allows the Chinese intelligence community access to every phone call, every text, and every internet search conducted through those networks. It can do so using data interception via back doors.

Even more alarmingly, equipment in these networks would allow China to control communication on connected devices. It could censor or alter communications, as it already does within its own national telecom systems. It would even be possible for China to shut down communications as a means of holding nations and economies hostage or as part of a war plan. Imagine being unable to call 911 in an emergency or open the front door of your smart home; imagine your doctor being unable to operate connected medical equipment or farmers being unable to harvest their crops with automated equipment. China's ability to dictate the terms of

connectivity has real life-or-death consequences. This might explain why this competition is so important and why competition over Huawei and Chinese networks is one of the few areas on which both political parties in the United States agree.

It's not that networks didn't exist before the fourth intelligence revolution. Spies regularly eavesdropped on communications during World War II. Most famously, British intelligence was able to intercept German communications that had been encrypted with Enigma machines and decrypt those communications using the first computers under the ULTRA program. The Cold War was rife with SIGINT, as was the post-9/11 world. The difference is that, today, networks play a much more significant role in our lives and in national security, with most of the world connected on these networks and almost all national security information passing through networks at some point.

Whereas networks were once the means of intelligence collection, now they may also be the ends. The NSA reportedly infiltrated Huawei to find out what the company was capable of doing with its telecommunications equipment, how it worked with the Chinese People's Liberation Army, and how to infiltrate these networks itself. The Chinese are no doubt doing the same to our networks. In the 2024 presidential election, it was reported that China had targeted the phones of both the Trump and Harris campaigns.

China and the United States vie for ownership of these networks because whoever controls them will have a major competitive advantage in intelligence. Nearly all intelligence transmits across networks at some point in its cycle. Indeed, most of our lives are being captured in these networks, from our social lives to our work and economic lives to how our government is run. Networks underlie all the traditional political-military areas of national security. Diplomatic cables must be sent over them. The military sends orders and sensitive weapons information across networks. Networks also underlie nontraditional areas of intelligence, like economic, S&T, and any other open-source information areas. Financial information is transmitted around the world for markets. Almost all scientific information is kept on networks. Control over these networks means control over all information.

Ultimately, this is a competition between political systems that control these networks, a democratic one where the rule of law matters versus an authoritarian one where the party may do anything it wants. There are checks and balances in place on U.S. usage of networked communication, as there are throughout the U.S. governance process. Laws and policies, congressional oversight, and judicial rulings all govern how U.S. agencies can deal with American information. Journalists and the media also play a role in these checks and balances by reporting when there are breaches to these rules. And, ultimately, the American people have a say. We can vote out of office politicians who do not conform to our ethical expectations. Previous revolutions in intelligence have been marked by limits placed on intelligence, from the dissolution of the OSS by President Truman to the Church Committee investigations of the CIA.

None of these checks and balances exist for authoritarian governments. If the CCP or another authoritarian government controls a network, it can do whatever it wants, whenever it wants. There are no limits to what it can do with data, people do not have privacy rights, the press cannot report on breaches, and there is no real way to remove a government that citizens disagree with. When you consider the issue of network intelligence in these terms, the choice is clear: we must compete to ensure that we control networks while also maintaining the rule of law over how those networks are used.

Networks are now an integral part of the Great Game of global intelligence. While control over them is the concern of our government, what should concern all of us is what these networks are used for beyond what is immediately apparent. They are the delivery mechanism for a perfect form of global surveillance of which Big Brother could only have dreamed.

OceanofPDF.com

14

Eyes Everywhere

In the 1974 Francis Ford Coppola masterpiece *The Conversation*, Gene Hackman plays Harry Caul, a surveillance expert charged with eavesdropping on a conversation between a couple as they walk around a park in San Francisco. As the couple walks, Caul must frantically direct and redirect his long-distance listening antenna to track them and then, later, painstakingly piece together the dialogue to understand their conversation. While Caul is a private investigator, his demanding methods illustrate the difficulty and complexity of surveillance during the second intelligence revolution. In this era, surveillance was an art practiced by experts using special tools, with very limited uses and in only the most important situations.

Over time, intelligence agencies improved surveillance technologies like listening posts, wiretaps, and satellites peering at us from space—as seen in another Gene Hackman movie, *Enemy of the State*. Here, Hackman plays Brill Lyle, a former NSA officer who is suitably paranoid as he tries to warn lawyer Robert Dean, played by Will Smith, about the surveillance capabilities available to rogue NSA agents trying to capture him. In this movie, corrupt NSA officers have access to ever-present surveillance from Dean's cell phone or satellites. These intelligence agencies could deploy their all-seeing surveillance systems to track anyone, from terrorists planning an attack to spies trying to steal secrets. But in this version of third-intelligence-revolution surveillance, it is still the government that maintains the surveillance system. This system is highly secret and centrally

controlled, and it remains a big deal to turn that surveillance system onto a target.

Today, during the fourth intelligence revolution, surveillance is neither particularly difficult nor the sole purview of secret agencies; it is ubiquitous, widely available, and targeted at all of us. We are all constantly and permanently under surveillance. This surveillance comes from private companies that own and operate the sensors and networks we all carry around. As soon as you awaken and turn the alarm off on your cell phone, the phone monitors you with over a dozen different types of sensors. You constantly carry around a camera, microphone, accelerometer, and myriad other sensors packed into a neat black box. Even without that phone, as soon as you leave your front door to head to work in the morning and walk toward a busy street corner, you might see a traffic camera. As you walk by the ATM, another camera stares out at you. Buy a pack of gum at a convenience store, and there's a camera up at the cash register, too. The Uber you take to happy hour after work has one. Every person you pass has their own device, which might catch you as you walk by or talk to them. Every website you visit or app you turn on records your every interaction and streams it back to databases. The refrigerator at your office might have a camera or other sensors within it that are streaming back to another database.

If *The Conversation* were made today, it would look far different. Caul would more likely access the microphone and camera from the couple's phone, perhaps through a cyberattack. From there, he might hear not only that fateful conversation as they walk in the park, but also everything they say to each other for days or weeks. He'd know precisely where they walked or rode in cars, when they intersected on the street, what they had for dinner, whether they'd slept together and for how long. He'd likely be able to even distill their plans and intentions as he analyzed their search patterns, what they were reading, what texts or emails they'd sent and received, or what social media they were following or posting. Caul would even know whether they were nervous as they said some of these things, perhaps whether they were lying, as their heart rate jumped on their smartwatches. If the couple, perchance, left their phones at home, he might

still access the phones of those around them, the streaming cameras, the apps and GPS in their cars, or even the commercial satellites flying over.

That said, good old-fashioned human surveillance still exists. In fact, for a period, I was one of those surveillants. We worked in teams, radioing each other to hand off our targets as we followed them on foot or in cars. It's almost like a sport: the longer you keep the target in sight without their knowing, the more points you earn. Except, that target isn't just another player; maybe they're a spy stealing nuclear secrets or a terrorist casing their next suicide-bombing target. The game's rules are much the same as they were fifty or even a hundred years ago: Be discreet. Follow at a distance. Hand off to your teammates if you feel burned. Remember: the targets are a slippery bunch, so stay focused. But this type of surveillance is becoming niche, like horses in a world of cars. It's reserved for the most important targets. Today, surveillance, like most things, has largely turned to technology.

Ubiquitous technical surveillance, or UTS, is the dry government euphemism used to describe the problem of this constant technology-based surveillance for intelligence agencies. The issue has been known within intelligence agencies for years, but it was most notably named in a 2022 speech by then CIA Director William Burns, when the former ambassador noted that UTS was causing agencies to fundamentally rethink intelligence. The idea is that various forms of sensor technologies can be used to surveil targets, not in snapshots, but all the time. This is just as scary to intelligence agencies as it is to you.

Closed-circuit television, or CCTV, cameras are what many of us associate with surveillance. Indeed, the image of a boxy white video camera attached to a wall has become symbolic of being observed. Once rare and dependent on teams to monitor them, these cameras are now everywhere, continuously monitored by AI systems that can flag suspicious behavior in real time or provide footage for reviewing a person's movements after the fact. Many cities, including Beijing and London, are reaching a point where cameras overlap across the entire city. One security company estimated that there are around 900,000 CCTV cameras in London, of which 35,000 are government cameras, plus 24,000 body-worn police cameras, and that

people are caught on video around seventy times per day on average. China may have a billion or more surveillance cameras—more than one camera for every two people. Instead of counting the streets under surveillance, it is easier to count those that are not.

Cell phones function as constant surveillance devices, enabling governments and companies to track your location at all times and, often, your activities. Beyond just a camera, microphone, and GPS, modern smartphones also include accelerometers, allowing them to know what you are doing, whether it's sleeping or exercising. The LIDAR, or light detection and ranging, sensor on your phone (similar to a radar, but using lasers) can create a three-dimensional map of the room you're in. And there are all sorts of ways to creatively use these sensors. For example, researchers have shown how it is possible to determine a user's fingerprints by the sound of their swiping on a smartphone screen. It probably comes as no surprise to you at this point that your phone can be used to surveil you. But what may be of surprise is just how much data can be gathered, not only from the camera and microphone, and that this data can be gathered even if you think your phone is turned off. Deleting data from your phone (or any other device) doesn't necessarily make it inaccessible; all that information can still be retrieved.

Computers and smartphones are not the only devices now collecting data. A much larger set of devices, known as the Internet of Things, or IoT, is also a vector for surveillance. These are the collection of all the smart devices that contain sensors and networked technology—smartwatches and fitness trackers, home automation systems like Alexa, industrial and agricultural tracking sensors, smart refrigerators, and other similar devices that are now ubiquitous in our personal, commercial, and industrial lives. IoT devices are already used by billions of people tacitly, whether they know that data about them is collected constantly or not. And these devices are growing exponentially, as more and more items in our lives are connected to the internet. Two trends will only serve to increase this growth: the proliferation of 5G telecommunications, which is built to more readily connect IoT devices, and the proliferation of internet from space.

Starlink and similar services will make it much easier and cheaper to connect devices outside wired or cell phone range.

An area of surveillance that many people don't think about is coming from space. Already, commercial satellite operators take images of the entire world every day using hundreds of small satellites. New satellites are on the way from companies that will be able to take images that are ten centimeters, which is high-enough resolution to see and, potentially, identify individual people. We already have the technology that produces images of the Earth using radar beams that can see through clouds and at night and are used by governments and businesses to monitor natural disasters, track illegal activities, and plan military operations. Still other companies provide hyperspectral data, derived from remote sensors that obtain the color spectrum for each pixel in an image, which in turn enables the viewer to identify the components of gases, liquids, and solids. Combine all these ways of sensing, and we will have an unprecedented, comprehensive way to look at the planet in its entirety at any given moment—to see traffic in real time; track deforestation or pollution; monitor resources and their distribution; and see if a country is urbanizing or preparing for war. As these satellites proliferate, everything on Earth will be viewable at all times—a moment referred to by the federal research center the Aerospace Corporation as "the GEOINT Singularity."

It is not just the ubiquity of surveillance that matters. What also differentiates the world of today's intelligence revolution from that of Harry Caul or Brill Lyle is who owns and operates the surveillance capability. Most surveillance collection is now done by private companies. Your cell phone is made by a private company, and its data is transmitted over private company cellular networks and fiber-optic cables to another private company's databases. Most satellites in space are owned by private companies. Governments still own and operate collection systems, such as massive radars and advanced satellites, but these are small numbers compared to the sheer amount of information available from commercial systems.

We are all surveilled. What varies is who has access to the data and to what degree they can tie the pieces together. Companies have some of the

pieces, and governments have others. In the United States, we still retain rules, laws, and norms that keep many of these pieces of data separate. In Europe, the European Union and national governments have instituted a more regulated approach, limiting what companies can collect, though national governments often face fewer legal barriers when collecting citizen information. In China, there are no constraints, but Chinese intelligence and security agencies still remain limited in what they can access in other parts of the world, where others control the means of surveillance or have laws in place to limit them.

One of the ironies is that the U.S. government has access to relatively little of this data for Americans. While the NSA has a reputation for monitoring everything you do, the reality is that there are strong legal protections in place and a culture of intelligence officers' staying out of the daily lives of Americans. Tech companies jealously guard their data. Moreover, the corporately collected data is dispersed around hundreds or thousands of different companies and, within them, across thousands of databases. Of course, the government may subpoena some portion of this data, and in other cases, it can purchase some of it directly from data brokers, though new rules are limiting that as well.

Ubiquitous sensors might seem like a boon to intelligence agencies, which are in the business of collecting and analyzing information. All agencies want this data, from the CIA to MSS to FSB to Mossad. Within their own countries, they can access much of the data through legal means. Externally or with foreign companies, they may need to obtain it by hook or by crook, stealing it with cyberattacks or simply bribing an employee to hand over the server.

But all this data collection is also a serious threat to those agencies' operations. For one thing, it is now very difficult to operate as an intelligence officer in the field, because everything, everywhere, is constantly monitored, recorded, and analyzed. It's not as easy as just turning off a cell phone or leaving it at home—doing so is itself a de facto admission of potential guilt. If I were a counterintelligence officer tracking someone, and they randomly turned off their cell phone for two hours at a time whenever they left the embassy, I'd certainly think they were an

intelligence officer. Nor can an intelligence officer just delete their Facebook account, sign up for a new one, and pretend to be someone else. Data doesn't disappear; it is simply stored somewhere else or underlies new data written over it. Re-creating a lifetime of social media and other data is very difficult. Again, if I were an investigator in Russia and noticed that a twenty-seven-year-old embassy consulate officer had no social media presence, when everyone else at the embassy had a lifetime's worth of embarrassing pictures on Facebook, I'd be extremely suspicious.

Taking a step back—there are two ways agencies can adapt to a world of ubiquitous surveillance. One is to fight technology with technology. The other is to adopt a change in mind-set.

The Intelligence Community now faces the daunting task of analyzing an astronomical volume of data from an ever-diversifying number of sources. Human analysts can handle only so much. Software and data systems have multiplied analyst capabilities, but they've been unable to keep up with even just classified information. Commercial and open-source data are growing at an exponential rate. Given the sheer amount of information, no number of analysts or traditional software tools will be able to handle processing that much data. As in the commercial world, AI is the only practical tool to manage it.

Adversaries are leveraging this data to spy on us as well, meaning agencies must now consider technology-based counterintelligence. Traditional methods—like hiding secret airplanes from satellites by concealing them under tents or using cybersecurity tools to protect databases from hacking—are already in place. These were hallmarks of the second and third intelligence revolutions.

Fourth-intelligence-revolution counterintelligence requires disrupting the patterns of activity that can be deduced from the huge amounts of surveillance data being sucked up by our adversaries. Their open-source intelligence collection may not obtain classified data per se, but by putting together lots of unclassified data, they may still uncover sensitive information by connecting the dots. The patterns of activity of embassy officials could be used to figure out who is a case officer. Social media could be used to determine order of battle by tracking soldier movements

and examining their pictures. The idea is not to be invisible but, rather, to be innocuous and ignored. Rather than a focus on clandestine intelligence (meaning “secret”), we may need inconspicuous intelligence (meaning “unnoticed”).

Counterintelligence must use equally powerful technology. This might include collecting the same information to determine the pattern of activity and then making changes to protocols to change that pattern. Or it could mean deleting information from or entering disinformation into available online data to disrupt adversaries trying to discern patterns and make predictions. It might mean hacking into their surveillance systems and changing data or other, more covert, approaches. These are actions agencies can take to deal with surveillance, but there is something more fundamental going on—not just a change in process or operations but a transformation in how to think about intelligence.

Agencies need to rethink intelligence because surveillance does not capture just a moment in time; it now captures people’s entire lives. We are moving toward a reality where everything you do, from birth onward, will be collected, turned into data, and stored indefinitely, potentially accessible to those with the financial resources, connections, or capability to get it. To practice intelligence in such a world requires thinking more like an insurgent. The communist revolutionary leader and chairman of the Chinese Communist Party Mao Zedong noted that the guerrilla must move among the people as a fish swims in the sea. Today, the intelligence officer must move among lifelong surveillance as a fish swims in the sea.

Even basic concepts in intelligence, like cover, need to change. Intelligence officers have long operated using fake identifies. But when a person’s entire life is now available to adversaries, they cannot easily create a cover. Rather, a person may need to live their entire life in a sort of quasi-cover. They may never even go to CIA headquarters or any other government building, for that matter. They might not be a paid government employee at all. It’s possible that physicists or start-up employees will work part-time as intelligence officers, rather than the other way around. This means blurring the lines of what it even means to be an intelligence officer

or a source. They must come to assume that surveillance is ever present and always operate within that surveillance bubble.

This vision of a radically different form of human intelligence is not unprecedented. During World War II and the Cold War there was another, more secret and essentially private intelligence agency called the Pond that operated much more commercially. The group was the brainchild of Jean Valentin Grombach, an eccentric French-American Olympian turned soldier. Grombach served under General Donovan in the COI and then was assigned to set up the Pond as a secret agency, separate from the OSS, in 1942. This new agency went on to run human intelligence sources globally in support of the war. The Pond was funded by the Army during the war, then the State Department after the war and finally the CIA. Ultimately, the CIA did not like the idea of a competing agency and had it shut down in 1955. Most interestingly, the Pond heavily used commercial cover, including not only having companies provide cover but even funding some of their operations. The organization eventually ended up operating as a private company that was funded yearly by the government. Ultimately the time was not right for the Pond's commercial approach to intelligence, and the CIA's much more robust centralized approach won out, but it may be that today is the right time for a highly secret, very commercial approach to HUMINT operations.

An intelligence officer envisioning the future from the early 2000s would hardly recognize today's landscape. Social media barely existed, and the concept of hyper-targeted disinformation campaigns on entire populations was incomprehensible. Supercomputers were confined to national labs or maybe to the bowels of the NSA, not available to anyone with an Amazon Web Services account. The idea of a venture capital–funded start-up with hundreds of surveillance satellites would have seemed laughable. Yet today these are realities for the Intelligence Community—which nonetheless possesses a key defense against such surveillance, one rooted in mind-set and that can benefit you as well.

★ ★ ★

Today, many of the things I learned at the Farm are as outdated as the flip phone I carried in my pocket at the time. The notion of who an intelligence officer is and what they do on a daily basis has changed dramatically. The Farm was created to conduct Cold War intelligence, that is, highly secret, long-term operations like recruiting sources, gathering human intelligence through manipulation, or plotting out dead drops—all the stuff of spy movies. Training for that kind of work doesn't always make sense today, when intelligence isn't necessarily secret, when human contact isn't necessarily required most of the time, and when there may not be a surveillance team to follow you because you are always under technical surveillance. Though the world of intelligence has radically changed, what endures is the intelligence officer mind-set, a way of seeing and thinking critically about the world. This attitude matters more than ever in the era of the fourth intelligence revolution.

A core lesson at the Farm is to focus on operational security, or OPSEC. Security is essential for any operation, whether it is having a meeting with a source or using a piece of covert communications equipment or passing through security at a foreign airport. Is anyone monitoring this meeting? Is this the best way and time to use my communications system? Can anyone see me logging in? Do I have a solid cover story? In a world of constant technological surveillance, the focus on OPSEC is crucial, but is challenging to execute.

There's no formula for operational security or for intelligence operations in general. The answer is always "it depends"—on the situation, the source, local security, your personality, and what you need to accomplish that day. Looking at security this way allows you to be agile, take calculated risks, and find something that works in that situation. This mind-set applies to any intelligence operation anywhere, from a chaotic war zone forward operating base in Helmand Province, Afghanistan, to a cushy embassy gig in Paris. It also means that no matter how technology changes, you can always adapt.

The Farm uses a unique approach to training people to think about intelligence operations, guided by experts with diverse field experience who can distill core lessons and ways of being that fundamentally shape your

thinking. It's a painful path of mentorship. Because the answer is always "it depends," the teaching method is to analyze everything you do and highlight what's wrong with it. You are constantly—and I mean *constantly*—being critiqued. There is no winning, and you need a thick skin. To think otherwise is "unsat," as they say there.

But, in the end, you develop your own inner instructor—a voice in your head that constantly questions everything you are doing everywhere you are. You examine choices about what you say to a source, whether to take a turn down road A or road B, or how to plan an operation. Then you question and requestion these choices. You internalize this way of self-critique. This is how you learn to operate alone, no matter the circumstances or what goes wrong.

Taking together this OPSEC mindset and "it depends" attitude means adopting a new approach to surveillance and realizing that it is not about trying to detect or evade surveillance. Rather, it's about coexisting with it while balancing the associated risk. There is no need for surveillance detection when you are always under surveillance. The task becomes determining how to maintain security and be clandestine while under surveillance. Operating in this environment alters the entire concept of OPSEC. There are techniques to detect and exploit gaps in surveillance, but in the absence of gaps, new methods of human intelligence operations will be necessary. This will require a deep understanding of tools like facial recognition and how to bypass that system. Human intelligence will become a highly technical profession and a team sport.

This is about learning to live with and within surveillance. Agencies have very specific ways of dealing with ubiquitous technical surveillance, though I won't get into the details. Protecting those secrets is important because they save lives.

★ ★ ★

It is not just intelligence agencies that must learn to protect themselves in a surveilled world, it is all of us. The Chinese Salt Typhoon hack demonstrated that their pursuit of a global panopticon is not only real but can target anyone, anywhere. The pursuit of our own surveillance system

during the chaotic intelligence age after 9/11 created the outline of a panopticon, which China has parasitically turned to its own geopolitical purposes. We laid the seeds of our own vulnerability. Now, we must turn to our own personal defense against this surveillance. In essence, that means learning counterintelligence tradecraft and practicing it daily. We can take some lessons from the Intelligence Community's ubiquitous technical surveillance mind-set shift to think about what you can do in a world covered in ever-present technical surveillance.

First, we must accept living with surveillance, rather than pretending we can escape it. It is impossible to avoid without disconnecting from society and becoming a hermit (and even then, your mountaintop hut would still be visible from space). Realistically, few of us can live without a cell phone or the internet at this point. The better bet is to learn to live with surveillance by thinking like a spy.

Thinking like a spy means creating your own personal OPSEC voice in the back of your mind that reminds you about security. You don't have to go to the Farm to do this. Just remind yourself to take a second and be aware of what you are doing; ask yourself if it is the safest thing. The next time you are posting something online, take two seconds to look at the picture or what you are writing. Does it give away anything you might not want it to? What might seem harmless—say, a photo of your bedroom—could have important information in it. Imagine a criminal using that image to determine what valuables you own and whether your window is unlocked. What about that post on LinkedIn? Make sure it doesn't reveal intellectual property that could be used by an adversary's military machine or make you a target. These two seconds can make all the difference.

Thinking like an intelligence officer is also about adding cost, making it harder for the adversary to target you. Espionage is a competition, and even when you are on defense, you can be on offense. For example, an easy way to protect yourself is to encrypt your communications, because encryption keeps your data safe even if a network is compromised. The Salt Typhoon hack by China intercepted only unencrypted calls and texts. By using Signal or another encrypted communication app, you can protect yourself by making it much harder for others to read or hear the content of

your communications. Ironically, during the third revolution, the FBI argued that the United States should make strong encryption illegal, but after the Salt Typhoon hack the U.S. government told federal employees to use third-party encrypted applications, like Signal, for personal communications because of vulnerabilities from the Chinese hack.

You can also mitigate risk by splitting up your data, and thus your patterns of activity, across multiple avenues—for example, by not using the same ecosystem of software and services, but instead switching between browsers or devices. Basic cybersecurity hygiene is also helpful, like changing passwords or being aware of phishing emails, because they add cost and time to adversary plans.

These sorts of operational security measures make it harder to target your activity because they force a bad actor to use more advanced means to hack you or to obtain data from multiple locations. None of this is bulletproof, but it increases difficulty and reduces your chances of becoming a target. But remember, this is a snapshot in time, so technologies and threats will evolve tomorrow and require new counters. Accordingly, stay focused on the mind-set rather than the specific technologies.

Finally, thinking like a spy also means prioritizing what information you want to protect and from whom. Some things matter more than others, and it’s up to each of us to determine what those priorities are. Criminals frequently target our financial information, and that is often people’s biggest concerns. But also keep this in mind: that information is the easiest to insure against. It’s likely your credit card already provides some form of protection or guarantee if there are illegal transactions, for example. Other people worry about personal information such as their Social Security number. But I’ll tell you right now, it’s highly likely your Social Security number was stolen long ago and is already available on the dark web. Yet few of us think about our political information or our health information. Authoritarian adversaries are targeting your political information for disinformation campaigns. It’s the same with your health information, including your mental health information, which may one day be used for all sorts of nefarious purposes. Protecting that sort of information from criminals and adversarial intelligence agencies is, in my view, of the utmost

importance. It’s not just for your personal privacy, but also for the safety of our families, communities, and nation. In the end, a stolen credit card number can be fixed, but a stolen democracy cannot.

The overarching goal I’m suggesting is this: don’t isolate or disconnect yourself. Instead, recognize threats and take precautions that are realistic. When people express surprise that I use an Alexa, I tell them it’s because it doesn’t really matter—I use a cell phone with a microphone on it, just like on an Alexa. If I’m not going to live with a cell phone constantly in my pocket, it makes little difference if there is another microphone in my living room. However, I make a point never to share my son’s information online, and where possible, I try to protect my own personal information, such as my whereabouts or photos of my home. We each choose where to be on the privacy spectrum, and we can make these decisions while thinking like an intelligence officer. Try to prioritize and secure what you can, add costs to those who might try to target you, and look at every situation with the OPSEC mind-set. We will never be able to escape surveillance, but we can learn to live with it and make the right choices to minimize its risks.

The rise of ubiquitous surveillance is alarming. What’s even more concerning is how this surveillance is used. Knowing information is one thing. Manipulating that information is another, and that’s where the next danger lies. This is another facet of the fourth revolution in intelligence, where technology is driving new types of intelligence and covert action, beginning with cognitive warfare but expanding into something much more terrifying.

OceanofPDF.com

15

Cognitive Warfare

In early 2004, no one would have believed that a website cooked up by a Harvard student to rate the attractiveness of incoming freshmen would one day become a major security threat to nations around the world. And yet, in 2016, Facebook was one of the primary weapons that Russia used to attack U.S. democracy.

Facebook wasn't the first social media site. Friendster and MySpace, two early digital social networking start-ups, used then-new technology that allowed users to easily create, upload, and share various forms of media. Facebook, Twitter, and YouTube formed shortly thereafter, where users had profiles and could upload videos, post personal updates, and share all that with other users. Through connections made in real life or online, people started receiving both personal and global information online. By the late 2010s, over half of people in the United States received their news from such sites.

Silicon Valley had unwittingly perfected a delivery mechanism for disinformation—and our adversaries were watching. By the time the IRA pumped its viral messages about the United States' 2016 election through every major social media site, including Facebook, Twitter, YouTube, and Google+, the scale and the means of manipulation were truly mind-boggling. Russia had learned quickly how to use algorithms to burrow into voters' feeds and their minds, preying upon a perception of trustworthiness. China watched intently and soon would unleash an even better social media disinformation weapon.

Standing on a dusty track in Iraq a decade and a half ago, with my rifle loaded and a source in waiting, I never would have thought that the biggest threat my nation would face would come from sixty-second videos of teenagers lip-synching and performing the latest dance moves—but here we are.

When you go on TikTok, you see videos of teenagers doing their makeup, kids imitating pets, homesteaders talking about their chickens—a more or less infinite number of videos that seem to have very little to do with the great power competition, let alone intelligence. How is it possible that such an app presents any threat whatsoever?

Yet two presidents, a few hundred members of Congress, several states, and nearly every national security expert in the United States have done everything they could either to ban or, at a minimum, to force China to divest from this app. In April 2024, President Biden signed a bill banning TikTok unless its Chinese owner divested from the company. And the United States is not alone: India banned TikTok years ago, as have other countries.

The question is why do these presidents, senators, and prime ministers all think TikTok is so dangerous? The answer to this not only illustrates why the U.S. government was right in its call for divestiture, but also why any similar app owned by any authoritarian nation must be banned to ensure the functioning of a democratic society. The simple answer is that TikTok is the ultimate covert influence Trojan horse. It can be used not only to spy on people's information, but also to control and manipulate information.

The threat is about more than a specific company or a specific app. The problem is around not only what the app can do, but also who owns it. When any powerful technology is owned by a company in an authoritarian country like China, it can and likely will be used by that authoritarian country for nefarious purposes. It's essentially the same problem as the Chinese-owned Huawei having operations in America.

While TikTok is one of the first widely popular social media apps owned by an authoritarian nation, it will not be the last. Seeing these threats helps illustrate how technology can be used by adversaries for not only

spying on people but also manipulating information and attacking whole societies. For this reason, it is worth diving in more deeply to understand how TikTok works and how it can be used for espionage and information attacks.

TikTok is the video-based social media app owned by the Chinese company ByteDance. In 2017, ByteDance acquired an American company, Musical.ly, to combine with its existing Chinese app Douyin. It then spent billions of dollars to acquire users through advertising on its competitors' apps Facebook, Snapchat, and others. Thus, TikTok could quickly scale—by 2024, it had more than 150 million users in the United States and over 1 billion globally. The app has been wildly popular with Generation Z, but if you are over forty, you may have never used it.

If you were to use TikTok for more than a day or two, you'd be astounded at just how good it is at recommending videos that match your taste. Most users will tell you that "it just knows what I like" or "they've got me dialed in." This is the notorious TikTok algorithm in action. No one outside the company and, really, no one outside China knows exactly how the algorithm works. No doubt it is an incredibly complex example of recommendation engine wizardry that includes core algorithms combined with thousands or maybe millions of optimizations. The result is a system that surpasses all others in modeling what you like and then sending it to you. That, combined with the sheer size of the user base, and therefore the amount of content available, makes TikTok a leviathan.

The means by which the algorithm works so well is also the first danger of the app. TikTok collects a huge amount of your data while you are using the app. ByteDance has even been accused of collecting data outside the app, including being able to access the microphone on your phone whether you are on TikTok or not, allowing it to record anything and everything you say. Anything you view, even for a split second, goes into its database and is essentially used to construct a model of you and your personality. That data might be vanilla, like which songs you prefer; or potentially more damaging, such as the fact that you might secretly be LGBTQ, or that you or someone in your family has a major medical condition, or what your genuine political views might be.

It’s true that many other social media platforms collect similar data, but those platforms are likely owned and operated by American companies or at least companies in other democratic nations. When a platform is based in a country that is governed by the rule of law and maintains basic freedoms, there is some level of regulation and legal boundaries over what can be done with your data. There is no such protection for the data in the hands of an authoritarian state like China. This makes it a fundamentally more dangerous thing.

The crux of the issue is that all that data can and almost certainly does go back to China. Since the uproar over TikTok over the past few years, ByteDance made statements about protecting user data and ensuring that it remained within the United States. However, it has been well reported that the data continued to be funneled to China. Remember: any Chinese citizen or company must provide access to data to the CCP if asked. But even if there were more protections, China has a long history of stealing data from U.S. databases, so stealing it from a Chinese company’s database would be trivial. This data can and will be used for some seriously concerning purposes.

Such data can leave people vulnerable to blackmail. Take Grindr, for example. Since Israeli entrepreneur Joel Simkhai founded it specifically for the LGBTQ community in 2009, Grindr has become one of the world’s most popular dating apps. By January 2016, it had ballooned to over 27 million users, and a Chinese company called Beijing Kunlun acquired it for $93 million. That sale created a significant counterintelligence threat, given that China could use the data to out or otherwise extort U.S. military and intelligence officers who use the app. The U.S. government was so alarmed about that possibility that it subsequently ordered the unwinding of the Grindr deal, rerouting the sale to a firm outside China.

The issue is not just about stealing data and using it for extortion. The TikTok algorithm that makes video recommendations is the perfect covert influence injection method because it can be controlled by the company. It is not just feeding you what is trending but can be manipulated to feed you whatever TikTok wants, in whatever volume it wants. And, since companies can be controlled by the Chinese Communist Party, this means that the

algorithm and therefore the information it sends to its users can ultimately be controlled by the CCP.

Not only is the app controlled by China, but such control has been actively used to promote or demote information aligned with CCP political messaging. In 2019, documents were leaked from ByteDance showing how the TikTok moderators were directed to censor information about the Tiananmen Square Massacre, Falun Gong, and Tibetan independence. The censorship led to deletion of the post, an outright ban of the person posting it, or other means of minimizing the post's spread by entering it into a category called "visible to self," in which no one but the user can see the post. ByteDance later noted that such policies had been changed, yet equivalent policies were still discernible through a study of what was posted and spread on the site.

The Rutgers University Miller Center on Policing and Community Resilience and the Network Contagion Research Institute published a study in 2023 that used a volumetric analysis of TikTok posts to demonstrate that the app was systematically promoting or demoting content on "the basis of whether it is aligned with or opposed to the interests of the Chinese Government." This systematic content bias was along hot-button topics like Taiwan, Tibet, and the Uighurs. The study's authors used the exact same methodology ByteDance itself had used in a previous study on whether it had a bias against Israel, by comparing the volume of posts between TikTok and Instagram, the social media site owned by the American company Meta. As the authors put it in one of their follow-up studies: "The results revealed a disproportionately high ratio of pro-CCP to anti-CCP content on TikTok, despite users engaging significantly more with anti-CCP content, suggesting propagandistic manipulation." These are just examples of bias and systematic information campaigns that we know of; there are likely many more examples of how TikTok has manipulated information.

Moreover, it has been shown that TikTok's propaganda worked and carried out Chinese Communist Party objectives. In another study by the same group in 2025 that built on its previous work, it was shown that TikTok was concealing information critical of the CCP and promoting information that conformed to its objectives and that TikTok users—

especially those who used the app the most—had more positive views regarding China's human rights record. This is compared to those using the American-owned social media sites Instagram, Facebook, and YouTube. In fact, there was a direct correlation between the amount of TikTok use and the degree of belief in the CCP message. This is statistical evidence that TikTok's covert propaganda machine works and is executing the CCP's geopolitical objective of converting the American public's views on China.

Putting these pieces together: First, the TikTok system can model what you like. Then the algorithm can direct any information to you that it assesses you will like and that it wants you to see. It can also halt information that goes to you that it does not want you to see. Much of the information you see might be harmless, but when desired by China, it could be tailored to a covert influence campaign. The controls of the system can be extremely subtle and manipulative, allowing for an optimization of influence. In other words, you likely won't even know that you are being manipulated.

This looks far different from the parasitic approach of Russia's Internet Research Agency. The IRA's covert influence campaign against the 2016 U.S. presidential election was a blunt instrument, a sledgehammer of obvious political messaging. It rode on top of the existing platforms and paid for this ride through the advertising system on Facebook and other sites. The messages that Russia sent looked and acted much more like traditional propaganda, with often over-the-top, obvious, or even ridiculous pictures and messaging.

By controlling the platform, the CCP can be much subtler and less likely to leave obvious fingerprints. For example, instead of using its own tailor-made political messaging to influence users not to vote, it might not make any content at all. Instead, it might push content in certain directions and for calculated reasons. It's about what content is pushed to whom and when. For example, the CCP might want to influence voting and so order the manipulation of content around concerns like "income inequality" or "immigration" or "human rights," perhaps in sincere and personal or witty videos. On their own, these are very valid concepts; indeed, addressing them may create a net public good. But if messages with this type of

content are targeted at users already known to be on the edge of not voting for a candidate, they could be used to influence them in a certain political direction or to not vote at all. This is strategic targeting aimed at undermining an election, just as much as what the IRA did in 2016, but without creating any content and leaving few fingerprints. Or if the goal is to weaken an industrial base in a particular area—say, to dissuade tech workers from taking what they perceive as threatening jobs, such as making AI that could be used in military systems—the platform might push homesteader videos to people on the edge of dropping out from the tech world in San Francisco or Austin and moving to the countryside. Again, there are no obvious fingerprints on this type of information attack, other than the manipulation of the algorithm.

The CCP can also use TikTok to control information by removing that information. It's not only the information that is pushed that matters; what is being minimized is just as relevant. This is what the Rutgers study demonstrated: that it was not only targeting content but also censoring it. TikTok moderators are tasked with banning so-called inflammatory content. But what is considered inflammatory in China is censorship in the United States, where we have a protected right to discuss political matters. By controlling the algorithm, the CCP (not ByteDance or its moderators) is able to enforce its political views on Americans and the world. China can remove stories so that they simply never come up.

Such censorship can be plausibly denied. TikTok could, for example, allow people to post and share information but then purposely and systematically underrepresent it through control of the recommendation algorithm. The drag on such information and stories pulls them away from people's attention. Again, it becomes hard to argue that TikTok is censoring information in that case, as the information can still be found, but the algorithm is minimizing the sharing of it for systematic, political reasons—essentially leading us right back to censorship. In fact, the silliness of TikTok content makes it even easier to plausibly deny its use as a covert influence platform because it can be hard to believe that such content carries messages.

Part of what makes TikTok so frightening is that its market dominance created an information echo chamber for an entire generation. More than three-quarters of Gen Z users (those born between the mid-1990s and the mid-2010s, the largest age demographic in the United States) used TikTok, and two-thirds of them used it daily. According to a Pew Research Center poll in 2024, nearly 40 percent of U.S. adults age eighteen to twenty-nine regularly got news from TikTok, up from 9 percent in 2020. TikTok thus became the de facto arbiter of what is going on in the world and what is real for a generation. During people's formative years, especially during high school and college, lifelong views are being formed and hardened. This is the time when values—whether personal, social, economic, or political—are developed. The TikTok echo chamber thus played an outsize role in determining young people's social, economic, and political values. Now, remembering that China can manipulate the information being delivered on TikTok, it's possible to see how it is thereby able to manipulate the views of an entire generation.

Of note, the CCP has banned American social media sites inside China and indeed even banned TikTok. Facebook, YouTube, Twitter, and every other American app are not accessible in China. As regards TikTok, there is another app owned by ByteDance, called Douyin, which is used in China. China has instituted legal monitoring and control over minors' use of social media apps like Douyin. It even goes so far as to limit the number of hours minors can be on social media and play video games and requires that educational content be provided.

Control of the platform is far more powerful than simply producing content. Instead of the blatantly political messaging of Russia and its IRA, covert influence packets on TikTok might just be funny memes, but targeted ones. Furthermore, since TikTok is the platform, it can and has enlisted its user base to defend the site, something the IRA could never do because the IRA did not have control over the platforms it advertised on and so was limited in what it could publish and how it could communicate with users.

China knows that establishing causality between content and behavior is hard, and maybe impossible, not only in terms of the covert nature of information operations but also in a democratic political environment. At

one level, it is difficult for politicians to make the case. Imagine a senator standing up in front of her peers at a hearing and presenting a homesteading video on how to take care of goats and arguing that it is undermining the U.S. military-industrial base. Or how could one prove a negative—say, that China removed or did not share information adequately, such as about Taiwan? TikTok's lobbyists and lawyers could easily argue that the algorithm just didn't find it interesting enough, and no one could prove otherwise. That is the point of well-run covert influence campaigns: even if they are exposed, they might be seen as just random or ridiculous or the object of conspiracy theorizing. You could think of this exploitative behavior as a sort of geopolitical gaslighting: try to call them out on it, and the Chinese will just shrug and protest that they are innocent, with a "who me?" or a "that sounds a little like a crazy conspiracy."

At another level, it is extremely difficult to censor any content or platform in America because the First Amendment protection of freedom of speech is extremely strong. Indeed, this is exactly where TikTok turned in its legal argument to dismiss the divestiture requirement. It's another example of China's parasitic threats. China treats the Constitution as just another tool for its national security goals—something to be exploited.

It can be difficult as an everyday user or consumer to decide whether apps like TikTok, or any other authoritarian government-controlled technology, pose a threat. The "proof" can sound circumstantial: data may flow into China, the CCP may have access to it and control over what packets are inserted. The connection between these packets and Chinese national security goals is soft. This is the innate difficulty of talking about covert actions when those actions have not yet been fully uncovered. However, operating in the gray area comes along with being an intelligence officer: you must deal with ambiguity and limited information. I hope the lens I am providing will allow you to read between the lines, see how the world of intelligence today really works, and make your own decisions, not just about TikTok but about any future app.

Regardless of the fate of TikTok, any information app controlled by an authoritarian nation should concern all of us. Anytime our information goes to an authoritarian government, we lose any control over it permanently,

and it is likely that government will use it against us for its own purposes. My hope is that the next time you see a new app or video game or AI system that comes out of China or another authoritarian nation, you will consider the consequences.

TikTok is one app that is aimed at generational information warfare impact, but there is something even more concerning. Education technologies, or ed tech, can sound innocuous, helpful even. These are apps that help students learn everything from languages to science. China is a leader in ed tech, where it is a $100 billion–plus industry. Indeed, even China's Douyin version of TikTok must ensure that a certain amount of educational content is broadcast. Maybe you imagine something like the Khan Academy, where millions of Americans have watched educational videos and learned something from them. But what is concerning is that China is focused on generational control of its own citizens and can use the ed tech apps to provide the education it wants, including political indoctrination. The democracy- and accountability-focused nonprofit Freedom House has, for example, pointed to how the CCP has been using surveillance, censorship, and indoctrination on its youth.

China's use of ed tech for political indoctrination will not stop at its borders. It is already pushing into Africa and other parts of the world. In 2024, Chinese vice-premier Ding Xuexiang announced a program to provide training to forty thousand teachers. Meanwhile, Southern University of Science and Technology, in Shenzhen, is setting up smart classrooms, including digital education—think ed tech—in thousands of classrooms across seventeen African nations. Also, Chinese companies like Tencent are investing millions in African ed tech start-ups.

If ed tech apps were to expand into the United States, they could be used as a spearhead to pursue covert influence campaigns through generational education and ideological indoctrination. The indoctrinating information could be hidden very subtly, making it, as with TikTok, hard to spot and plausibly deniable. Children would have few defenses against these attacks. Such threats are already on our shores. The tutoring site Tutor.com and the test preparation company Princeton Review are Chinese-owned and -controlled educational companies that have been used

throughout the United States, including by the U.S. military and millions of students in our nation. The threats from such technologies must be seen for what they are—means to collect information about American students and potentially ways to push political indoctrination messages.

Chinese-owned AI could be the most dangerous technology of all for U.S. citizens or anyone in democratic nations. AI will increasingly be the arbiter of information. Already, ChatGPT and similar systems like Perplexity are becoming the first point of search or questions for users. At the same time, it is difficult if not impossible to establish how such AI answers questions or from where it draws its conclusions. These systems could thus become the ultimate covert information operation vector by being biased toward a specific information, geopolitical, or security goal of those who control them. China already censors and manipulates information in AI systems that are used by its own citizens in order to execute social control of its own citizens. Within China this is done overtly and through regulations. Should such AI take hold in America, the Chinese would no doubt do the same here covertly.

Indeed, Chinese AI apps like DeepSeek are already here, and Americans must be wary. As expected, DeepSeek does censor information about Tiananmen Square and other hot-button Chinese political issues. AI will be even more dangerous than social media like TikTok. Hopefully, we will learn lessons from the danger of TikTok and inoculate ourselves from the next information control threat.

AI or apps like TikTok and Tutor.com are not the only form of information control used by China. Within China, using what is known as the Great Firewall, the Chinese government monitors and censors the digital activity of all 1.4 billion of its citizens. To control thought within the country, this firewall denies the Chinese people access to websites that promote anti-China ideologies. The list of what the CCP considers unacceptable is quite long, including sites like X and the *New York Times* and specific search words, ranging from “Dalai Lama” to “Winnie-the-Pooh” (whose pudgy face is sometimes used as a symbol to represent Xi Jinping). With the advent of new technologies like AI-based monitoring, this government control is becoming only easier. Ironically, China did not

create this system alone. U.S. tech giants like Cisco and Juniper Networks were contracted in 2004 to provide an upgrade that was used to expand the government's censorship abilities.

China's attempts to control information and communication go well beyond simply censoring information coming into the country. The CCP employs a strategy of actively combating antigovernment ideologies and forces both domestically and internationally. The United Front Work Department in the Chinese government runs foreign influence operations aimed at depicting the CCP in a more positive light, taps into sympathetic Chinese communities abroad, and can be used to repress dissidents. When propaganda does not work, the United Front and other Chinese government agencies have also physically threatened and assaulted protesters in the United States. It also works with organizations to develop and distribute propaganda, oftentimes on college campuses throughout the United States and the West. These organizations include branches of the Confucius Institute, the Chinese Students and Scholars Association, and the China Association for International Friendly Contact.

People seeing a Confucius Institute near their college campus might think it akin to Germany's Goethe Institut, an innocent means for cultural sharing; it is not. These institutes are explicitly part of a global campaign to influence foreigners' perceptions of the Chinese government. They restrict academic freedom at host universities by pressuring universities to avoid teaching topics sensitive to the Chinese government, such as human rights in China or Tibet. Confucius Institutes have also been suspected of being used for espionage or surveillance by Chinese students abroad.

China also strong-arms American public figures who counter their narrative. This has led to a dynamic in which Hollywood regularly self-censors its content in accordance with the CCP's guidance. For example, in the original *Top Gun* film from 1986, Tom Cruise wears a bomber jacket with patches of Navy tours, including flags from Japan and Taiwan. However, the Japanese and Taiwanese flags were removed from initial previews of the 2022 sequel to appease the Chinese government and market. Ultimately, those flag patches were returned to the jacket after the Chinese entertainment and technology company Tencent ceased being a

producer of the film. Similarly, during an interview with the Taiwanese news station TVBS, actor and wrestling star John Cena said that the first country to see his new movie *F9* would be Taiwan. Cena's acknowledgment of Taiwan as a "country" led to an uproar on Chinese social media and, ultimately, to a bizarre apology by Cena in Mandarin. China even went so far as to effectively censor a high school in Colorado for implying, during the school's Model United Nations sessions, that Taiwan was a separate nation-state. This is not the fault of John Cena, nor of the producers of *Top Gun*, nor of the Colorado high school. They are not the perpetrators. They are the victims of Chinese censorship campaigns that use the sway of an entire nation-state to force private U.S. companies and individuals to play by its rules.

The Soviet Union and Chinese communist governments used to painstakingly edit photographs to change historical events by removing the faces of those no longer in favor. Today, we face similar attempts to change history. While China attempts to remove the Tiananmen Square Massacre from its domestic history, it also tries to do the same thing to the United States, through censoring TikTok and with whatever other means it can. Such efforts to rewrite history are not, however, just about censorship.

★ ★ ★

These attempts to control information and influence people are part of a larger strategy of cognitive warfare. China has for years theorized about and pursued cognitive warfare. One way to think about this concept is that it is about convincing an enemy not to fight before the battle even begins, an idea going back to the Chinese political and military theorist Sun Tzu. Cognitive warfare can be aimed at everyone, from soldiers to individual political leaders to the general public. Disinformation is one means of pursuing cognitive warfare, as are denial and deception, or even the use of drugs administered to individuals to make them more pliable. It is a means to control how people think and what they think in such a way as to influence them to do what you want, whether that is a private surrendering on the battlefield or a general not attempting to occupy a city or an entire population being for or against a war. In other words, cognitive warfare is

about actively changing or even controlling how we think and act, i.e., mind control, and this is not science fiction, it is very real.

Cognitive warfare in the form of propaganda has always been part of politics and warfare. All sides released propaganda against the enemy and to their own people during World War II. By the time of the Cold War, propaganda had evolved into a global pursuit and into the idea of brainwashing. Indeed, a so-called mind-control race occurred during the Cold War in which the United States, Soviets, and Chinese attempted to develop means of manipulating the human mind in their ideological conflict. Most of this was pseudoscience. The idea was introduced to the public during the McCarthy era and, spectacularly, in the movie *The Manchurian Candidate*. Revelations by the Church Committee investigation into U.S. intelligence included that the CIA's MK-ULTRA program dosed innocent people with LSD as part of experiments in mind control. Of course, the Soviet and Chinese programs were never investigated and released to the public, but no doubt they pursued similar avenues.

Where LSD failed, silicon has succeeded. What is different today is that the internet, ubiquitous connection through cellular phones, AI, and huge amounts of sophisticated content have provided a means for society-wide cognitive warfare. Think of networks and apps as combining to form an entire disinformation superhighway directly from the Ministry of State Security to someone's mind. China has attempted to control the networks upon which this disinformation superhighway exists, as with Huawei. On top of those networks sit apps like TikTok, which can manipulate that information. Unlike the one-way disinformation paths of newspapers and television, these pathways are two-way. How people react to information is recorded and analyzed so that the messaging can be optimized.

Such cognitive warfare will likely go so far as to literally read minds and control the brain directly. A new breed of technology is already coming to market that uses sensors on the skull of a person to detect brain signals and then uses AI to read these signals. One study in the scientific journal *Nature Neuroscience* demonstrated how a functional magnetic resonance imaging (fMRI) machine combined with AI technology could be used to

generate “intelligible word sequences that recover the meaning of perceived speech, imagined speech and even silent videos.” In other words, to read a person’s mind. Neuralink and other companies are developing similar technologies that one day will allow people to integrate computers directly with their minds, where their thoughts are read directly and can be used to control machines. Already, there are multiple brain–computer interface (BCI) companies with products that use noninvasive sensors to, in effect, read certain brain patterns and control machines with them. Smartwatches and similar sensors are regularly used to measure proxies of the mind, such as by associating a person’s pulse with other information.

Brain information is ripe for espionage and cognitive warfare. Intelligence agencies will want to know what you are thinking. Ultimately, they might try to use this information to directly read a person’s mind. But even before that, the information could be used to determine whether a person is lying, as with a polygraph machine. Perhaps hooking someone up to a multimillion-dollar fMRI machine is not the most efficient means of intelligence collection, but doing so with a captured terrorist with plans for an attack in his mind might be a reasonable means of interrogation. But technology is moving quickly. Already, IoT devices like smartwatches can be used to measure blood pressure and other reactions and, thereby, serve as a proxy to mind reading.

It’s easy to see how such information can be used to invade a person’s mental privacy. For example, information about your mental state, such as your level of awareness or anxiety, could be correlated with an image you are looking at or a conversation you are hearing. This correlating information could then be used to determine whether someone truly is attracted to the gender they say they are, or believes in the god they say they do, or is really a supporter of a political party they say they voted for; or it could otherwise infer information about what they’d prefer to keep private. It’s hard to overstate what a nightmare breach of privacy this would be, especially in places where the answers to questions like these could mean imprisonment or execution.

Mind reading could also be used to better determine how a person is reacting to information and, thereby, to better tailor information attacks. In

fact, there is already an area of business called neuromarketing, where brain information is used to better tailor marketing and advertising. Tailoring a marketing message using brain information is only one short step away from tailoring an information attack. It's a safe bet that brain data is already being stolen from app companies, that intelligence agencies are developing technologies to read minds, and that, in the near future, even your private thoughts will be used against you.

Given the massive potential for an invasion of privacy, there have been moves to protect brain data. In 2024, Colorado and California passed laws that extended privacy protections to brain data. No doubt, other states will follow. This also means that our intelligence agencies should begin to see brain data as a vulnerability that should be protected. Counterintelligence must turn to protecting the thoughts not only of politicians, generals, and other intelligence officers, but also of millions of Americans.

Cognitive warfare is a means to affect entire societies across generations. Imagine, for example, a disinformation campaign on steroids, carried out over the course of years, targeting the American public in such a way as to convince them that the United States should not fight to defend Taiwan. The public might go on to elect leaders who promised not to defend Taiwan, and those leaders would ensure that military policy changed in that way. Perhaps the perpetrators systematically erase and confuse any history of American support for Taiwan from historical records, using cyberattacks to delete files and information attacks to obfuscate historical truth. Such a campaign might be generations in duration, addressing those in power today but also sending propaganda to younger generations as they grow, so that by the time they are in power, their views are already baked in and taken as a given. This is how China could potentially win the war for Taiwan without a shot being fired. We are in a generational competition that cannot be ignored and requires generational intelligence to win.

★ ★ ★

Today's intelligence agencies sometimes continue to think that their job is only to collect and analyze intelligence about political and military issues that concern presidents and generals. It can feel as if the Cold War

continues, as if it is the particular frequency of a radar signal or the machinations of a single colonel in a coup that will make the difference between a safe and secure United States and a threatened one. The evidence is there when you look at the size and budget of traditional political-military offices in the IC versus those focused on cognitive warfare–like activities. This is simply wrong. The safety and security of our nation is just as threatened by cognitive warfare as it is by bombs and bullets. The longer we continue to abide by this old view of national security and the role of intelligence, the more threatened we will become.

The fourth intelligence revolution is not only about collecting and analyzing intelligence; it is about controlling and manipulating information and people. Cognitive warfare is a key ingredient for this revolution, as are the technologies that underlie its delivery. Intelligence agencies were once focused primarily on finding out information and understanding what was going on in the world. Now they must focus on finding out how information itself is being manipulated. They then must help to defend against this information manipulation. The theorist Marshall McLuhan once said, “The medium is the message.” Now the medium and the message are both being controlled and manipulated by our adversaries. We must focus on this new medium of networks and social media platforms, and the unceasing transmission of information, as well as on the messages those networks and platforms carry.

U.S. intelligence agencies need to face this reality and build the capabilities to fight cognitive warfare. Cybersecurity is already a big part of defending against cognitive warfare attacks, but more must be done. Further investment begins with investing much more in the people and tools for understanding cognitive warfare attacks. These might include hiring experts and obtaining software from the marketing, advertising, and sociology professions, rather than from traditional political science areas. It definitely requires involving other agencies, from law enforcement and perhaps even the public health sector, that can address domestic issues and the American people directly. More generally, it means seeing citizens as the asset that needs to be protected, not at a general level of national security, but as the specific targets of attacks. Plans and procedures need to be developed for

protecting people's minds not just during elections or wars but continuously. Finally, we will need to address to what degree we want to take part in offensive cognitive warfare. While it may make some of us squeamish to consider any offensive operations, it is worth remembering that winning the war without a shot's being fired is not such a bad objective to pursue, and cognitive warfare is one way to do that. Whether we like it or not, cognitive warfare will be one of the fixtures of the fourth intelligence revolution.

This is a race of intelligence revolutions in which our adversaries have already turned the corner. Their own intelligence revolutions involve ever-present global surveillance, cognitive warfare upon generations of civilians, and dominance of a few key technologies. As Chen Yixin, the head of China's primary intelligence agency, the MSS, has said, "The Internet is the new battlefield and new media is the new combat power." Fortunately, this is still the first lap in the race. Nonetheless, leaders are sprinting out in front of us while we are held back by the weight of seventy years of history, bureaucratic acceptance, and a misunderstanding of the nature of the race. If we want to keep up, we need to change our perspective on what constitutes warfare, what it means to control information and people, and, in essence, even what we define as truth.

Surveillance and networks are only the beginning. The battle over information goes past the screen on your phone. Cognitive warfare is part of where this heads, but the rabbit hole goes much deeper. The combination of networking technology and cognitive warfare with AI will form a direct pathway all the way into your mind. This brings us to the final stage of the fourth intelligence revolution.

OceanofPDF.com

16

Hacking Minds

When ChatGPT 3.5 was first released to the public, I sat my then eight-year-old son down and told him he should remember this moment. We had the new AI system tell us a story about a dragon. Within seconds, it spat out a perfectly framed story with a beginning, middle, and end that could have been written by a person. We asked it to give a comparison of tigers and polar bears. The AI made cogent points about tigers and polar bears, written in perfect syntax. I cannot remember the exact first moment I logged on to the internet in the 1990s, though I wish I could, because the internet changed my life and most everyone else's. I wanted a marker in my son's mind of when he first saw a peak at how the world would change again.

My son is a member of Generation Alpha, the first native AI generation. Gen Z was the first generation to grow up with social media; Millennials, with the internet; and Gen X, with computers. Kids my son's age have been exposed to AI in some form since birth. It is reflexive for him to ask Alexa to turn off his light or to play him a song. Now with ChatGPT and similar large language models, it is normal for him to pose questions or make much more sophisticated requests. To their credit, his teachers have already introduced AI into their elementary school curriculum. The hope is that, unlike my generation, who, when learning math, were supposed to pretend calculators did not exist, he will grow up with AI as an integral part of how he learns.

By the time I joined the Intelligence Community, I expected computers to be part of intelligence gathering in a way that my predecessors did not. Similarly, Generation Alpha will certainly expect that of AI. In a decade,

they will be interning at agencies; and shortly after that, they'll be running operations and, eventually, managing the entire Intelligence Community. It will not be strange at all to my son that machines spy on machines for the benefit of other machines. The outcomes of the current revolution in intelligence will seem as commonplace to his generation as it now seems to email someone rather than send a letter or to search a database rather than pull a physical file out of a cabinet.

What I did not tell my son in our first foray into using ChatGPT was just how dangerous this new AI technology will be for him and his generation—not because of the theoretical dangers, like the idea that AI will escape and become a *Terminator*-like Skynet. That fear might be real, but there is nothing to lead me to believe we could see anything like a true independent and existentially dangerous artificial intelligence for decades. Rather, I'm more concerned by what is already happening. The very thing that makes this new crop of AI so powerful—its ability to find patterns, to understand information, to say convincing things—is what makes it so dangerous. In other words, what makes it so dangerous is that it can do what we as humans do, and that danger is already here.

★ ★ ★

Artificial intelligence will be used by adversaries to hack our minds. Intelligence agencies want to extract secrets from people's minds, and they want to change people's minds about how to behave, whom to trust or what decisions to make. It is inevitable that AI will be used as a tool to realize that mission.

In traditional computer hacking, information is stored within the computer and secured in some way. The hacker must figure out how to evade or dismantle that security system to get at that information. From there they can steal or change the information. Maybe they enter an account number to siphon money or they figure out how to disrupt the power system in a building to abruptly cut off the lights or steal a secret access code.

Hacking a human mind is not much different from hacking a computer. Information is stored in our memory, and it's possible to access it or change it, but doing so requires evading our security. Our mind's security system is

built around self-interest, distrust, and critical thought. We may not want to give up information because it is not in our favor. We may not trust someone or something that is said. Sometimes we are just skeptical: we have all been taught that we can't always believe what we see.

Self-interest is the easiest way to hack a mind, and it is a favorite tool of the intelligence officer. A person can be convinced to do something if it's in their favor or conforms to their beliefs. Perhaps they are shown how their ideological belief is best met through doing something—for example, maybe they fear nuclear war and are shown how sharing information about nuclear secrets will help limit the chances of one. Or perhaps they just want more money, and you can give it to them in exchange for secrets. Aldrich Ames was an alcoholic former CIA counterintelligence officer who committed treason and sold the names of CIA and FBI sources to the Soviets. He later said, "My little scam in April '85 went like this: Give me $50,000; here's some names of some people we've recruited." Fortunately or unfortunately, depending on which side you sit, sometimes it is that easy.

Overcoming distrust is more involved. Building trust takes time. Much of the work of case officers is about building trust by establishing rapport with your source, by illustrating how similar you and the source are, and by doing what you said you'd do. But there are shortcuts.

Trust can be built through repetition and simply spending time together. This is at the core of the advertising industry—show someone a brand enough, and they will trust it. Russia's 2016 approach to evading skepticism, as it manipulated the U.S. public in advance of our presidential election, was built around the advertising approach to truth and lies. Tell the lie enough times, and some people will hear it as truth. This has become even subtler and more pervasive since then, such as with TikTok. However, the problem with the approach is that, eventually, the truth will come out. As people start to see the lies and uncover the truth, they will turn to critical reasoning.

Critical thought is the toughest bodyguard our minds have. We all build a mental model of how the world works. Whenever we are presented with new information, we add it to that model. Maybe it fits and reinforces a

belief. Or maybe it doesn't, and it creates cognitive dissonance, a normal, rational reaction to not being able to hold contradictory beliefs.

Evading critical thought is a much subtler operation. It requires convincing someone of something, which involves a few steps: one, understand a person's mental model of the world (including their assumptions or premises); two, establish how this new information conforms to those premises and fits in; and three, change those premises by establishing a different or hidden premise that makes more sense to them than their original. Perhaps they believe the Sun revolves around the Earth because of what they have been told their whole life and because it sort of looks like that from the ground. But they also believe in logic. Then they are shown how it makes more logical sense that the Earth revolves around the Sun.

The thing about overcoming critical thinking is that it requires a dialogue. There needs to be a conversation. I suggest something, and you push back and say it's false, I come back with a different suggestion, and so on. This is straightforward enough if I'm a case officer and you're my source. I can convince you over time. But it's not possible to do so easily at scale simply by pushing more advertising.

AI changes this equation because it can enter a dialogue to build trust and change a mind over time. It is especially adept at this because it is great at pattern recognition. It can see how you act and react to information online by looking back on years of your data. It can assess whether you clicked on a link and whether you shared that information with others. Or it can see what minor changes to the way a message was delivered led you to do so. Beyond subject matter, maybe it was how creatively the story was written, or the tone of the content, or even just the placement of the Share button or the type of font used for the text that made you respond. In essence, it's possible to build a model of you, including how you act, react, take in information, and forward information back out. AI can thus optimize the information coming at you to best convince you to do something.

Analytics like this have been used to inform information attacks for years, but large language models like ChatGPT are a quantum leap in capability. Previously, creating new information required a human's

involvement: for example, the copywriters at the IRA. But now the system can be integrated in such a way that the AI can both assess what you respond to and also write that content itself. It thus creates a feedback cycle in which information is created and fed to you, your response is noted, and the next input fed to you is more according to your taste and needs, better optimizing the system. Instead of being based upon generalities derived from the behavior of groups of people, as advertising is, this information delivery can be truly tailored to you and only you.

AI is already evolving in the direction of being able to personally tailor its points and arguments for different types of people. For example, in an interaction I had with OpenAI's ChatGPT I asked the system about its voice, and it let me know that "it's designed to sound natural and conversational. It's meant to feel approachable, like you're chatting with a friend." I then asked it to sound less conversational and more formal. It then repeated the same phrase in the more formal manner, now noting, "My voice is … designed to convey clarity and naturalness in written communication. Its purpose is to facilitate effective interaction." It's subtle but you can see how tone can be shifted in ways that appeal to one personality type or another. Here is another conversation that shows how the system can be tailored to convince different types of people. My prompt:

> I am a person who responds well to authority, can you convince me that the world is round.

ChatGPT response:

Certainly. Let’s approach this with authority and evidence: The world is demonstrably round, based on centuries of observation and scientific inquiry. Here are key points to consider:

1: Photographic Evidence: Since the advent of space exploration, countless images have been taken of Earth from space. These photos, captured by astronauts and satellites, clearly show Earth as a spherical object…

Now, observe this second interaction where I request a different type of response for another personality type.

I am a person who responds well to softness, friendliness and understanding. Can you convince me that the world is round.

ChatGPT response:

Of course! Let’s explore this together in a kind and approachable way.

The idea that the world is round isn’t just a fact—it’s something you can see and feel in little ways every day. Here’s how:

Photos from Space: When astronauts go into space, they bring back amazing pictures of Earth. It’s a beautiful blue ball, glowing against the darkness of space. Those images are so full of wonder!…

These responses illustrate how AI systems can tailor their responses to a user’s personality in order to convince them of something by using different argument approaches, vocabulary, and tone. Such tailoring could be done for any type of personality or any type of question; it could be to

convince you to vote or to convince an intelligence analyst that an invasion is imminent. In my example, I prompted ChatGPT to use the different styles, but it's easy to imagine how an AI system could use an approach tailored to my personality without letting me know.

The tailored argument approaches are not limited to verbal communication. For example, OpenAI has released Sora, which is a video system. Through Sora and similar systems from other companies, videos can be created from scratch based upon a prompt. Such videos could be tailored to appeal to me as an individual. For example, a video showing a rebellion could be made in such a way as to make the people in it look like stoic freedom fighters or dark threats.

We are accustomed to propaganda, disinformation, and manipulation coming at us down a one-way street, but AI engages us on a two-way street. Rather than a bombardment, it is a dialogue. The more you say, the more you reveal about yourself, granting it more material to use. Even when you don't believe it, it learns from you and adapts. You might refer to something as "unbelievable" (i.e., you express cognitive dissonance). The AI could take that in and then change its argument. It might try to more subtly manipulate you, not through the message, but through talking about other things unrelated to the issue. Perhaps it never tells you that you should trust Russia, but it tells you a Russian folktale that expresses how trustworthy Russians are to their friends. Subtlety can be hard when you're pushing a message to millions, but in a one-on-one conversation, it's very feasible.

To summarize, the cycle then looks like this. An AI models you, creates information that will appeal to you, feeds you that information, gets feedback based on your reactions, updates the information, feeds you new information, and so on, repeating ad infinitum, in all domains of your life. And it is all done with the goal of convincing you of something or to do something.

Now imagine this discussion with AI taking place over a lifetime. This would be an AI that is tailored to you, your individual quirks and proclivities, your insecurities and weaknesses. Think about a multi-year conversation you've had with a good friend in which you didn't agree with them at first but were slowly convinced of their point of view. The AI will

also try to convince you from childhood. It knows how you think and what you are like. It will be more like you had a personal friend in the KGB, someone who knows you better than anyone else, but who is trying to recruit you all the time, everywhere you are, and very subtly overcoming your skepticism and defenses toward their goal. You'd have your own personal propaganda officer.

Perhaps it plays out something like this. You begin talking with someone online, perhaps knowing they are an AI from the start, but perhaps not. Either way, this being comes to know you better than anyone. They've read everything you have ever written, and maybe, eventually, through AR glasses, they've seen and heard everything you have ever seen and heard. This data about you and your life has been translated into a model of you, a second you, that the AI can now use to run scenarios. The system knows exactly what buttons to push to make you want something, to build trust, or to create what you consider to be a reasoned argument for or against a certain action. It does not necessarily need to make the argument at any point; perhaps it just shows you information that leads you in that direction. It might want you to believe that you came up with the idea yourself, like in the Christopher Nolan movie *Inception*. It gives you the information, not in a dream, but through a long-term strategy of drip-feeding true, false, out-of-context, or completely made-up information. It can also try to withhold from you information that might go against its argument. After a while, this becomes a closed loop of information, where anything that deviates has been pushed out, made inaccessible.

AI systems are so good at figuring people out that I fear we will not only be deeply influenced by them, but that we will also start to fall in love with them. In October 2023, a *New York Times* reporter described how his Microsoft Bing chatbot, whom he had named Sydney, tried to convince him to leave his wife. As AIs learn more about our individual desires and dislikes, they will become better than ever at anticipating what we want and how far we will go to get it. What about a partner who only wants to soothe, please, and support you, with no concern for their own ego. Someone who knows exactly what you want, what you need, before you do. The movie *Her*, in which Joaquin Phoenix's character becomes increasingly obsessed

with an AI he names Samantha, is not far off. Taking it a step farther, I can imagine a whole new world of therapists focused on people who have fallen in love with AIs. At that point, an AI system that convinces us to commit treason will seem trivial.

Everyone will confront these omnipresent AI propaganda machines. They might be used by companies to sell you something. More nefariously, these systems will be used by adversarial intelligence agencies to get you to vote in a certain way or to pass secrets or carry out generational information attacks. No one will be safe. They will also go after generals, CEOs, senators, and intelligence officers. Though these people may have better information, the AI may also be subtler in its approach to them, slowly injecting doubts to imperceptibly skew their views over time.

For you and me, it might be more difficult to overcome our years of experience and skepticism, but imagine this process beginning with a child. From the time someone is a toddler, there may be an AI model of them that not only gets to know them, but also shapes them. The primary determinants of a person's fundamental views, from their political leanings to their favorite sports team, have always been family, schools, and eventually friends. Books, radio, TV, and the internet begin to play a role, but again, as one-way streets. AI will become another player on this field. An AI propaganda machine could tailor itself perfectly, whether to personality type or interest area or age. Imagine it making very subtle hints and insinuations to a child when telling a story. Perhaps the moral of a bedtime story being told to the child could be geared toward developing a set of values that the AI propaganda machine wants—say, that authoritarian control is a safer form of government than chaotic democracies. These would be intergenerational information attacks.

Such mind hacking will be global because AI propaganda machines are highly scalable. They can produce as much content as desired. Back in 2016, the IRA had to hire more people to write more content if it wanted to continue tweaking and pushing out messaging. That's no longer the case with AI, which can tailor any amount of information to anyone. AI machines are also scalable in the sense that they can be assigned to every

person. It is just a question of the cost of compute, and with that cost coming down rapidly, it's a question that favors the propagandist.

These AI propaganda machines can be used for any intelligence mission an agency wants. They may want to get information from you; and over time, they will do so by slipping in intelligence-collection questions. Alternatively, the system might manipulate you to believe an adversary's propaganda, or it might assess and prepare you to be recruited by a case officer.

In this likely future of AI propaganda, we may not even know we are committing treason. Aldrich Ames was recruited and offered money for source information. It was a conscious act. But why not just skip this step entirely and convince you, slowly, over time, to leak information? You never meet someone from an intelligence agency, and you are never even asked to do anything. Rather, over time, you believe you came up with the idea on your own to leak secret information. You would be an unwitting source, and there would be complete plausible deniability for an adversarial intelligence agency. In fact, you'd probably still pass a polygraph exam, since you would not consider yourself a source and would have no knowledge of the influence of a foreign intelligence agency.

Perhaps the AI convinces you that your government is bad and that the only way to help your society is to steal data from your government job or your company's corporate database and then release it online. Or perhaps the AI could influence you to vote a certain way or not vote at all, or not to take a job developing autonomous weapons systems for the military, or take a positive view of the Chinese Communist Party. This is intelligence being done without intelligence officers.

This reminds me of Sun Tzu's adage from his fifth-century BCE classic *The Art of War*: "The supreme art of war is to subdue the enemy without fighting." The supreme art of intelligence is to recruit a source without recruitment.

China is at the forefront of the revolution in disinformation, as we saw with TikTok, and it has already begun using AI to further its information-control ambitions. In early 2024, for example, a group associated with the Chinese Communist Party posted AI-generated audio of one candidate in

the Taiwanese elections endorsing another. But this never happened. OpenAI itself acknowledged that "its generative artificial intelligence technologies [had been used] to deceptively manipulate public opinion around the world and influence geopolitics." Similarly, the Chinese AI model DeepSeek already censors and manipulates information. The vision I have laid out is not the distant future; it is happening now.

Hacking minds is the perfect culmination of the CCP's information control strategy. It will seek to create autonomous cognitive warfare. If for only this reason, the United States must ensure that no Chinese-made AI is allowed to enter the U.S. market. Preferably, Chinese AI should not be allowed to enter any democratic nation's market. But it will not be limited to China. Every intelligence agency will likely end up using AI propaganda, and so we must limit the authoritarian use of AI. Ideally, U.S. intelligence agencies and law enforcement would devote significant resources to trying to defend against AI propaganda machines. This is a much more dangerous issue than social media information attacks like those perpetrated by the IRA or TikTok because it is so subtle and convincing. But traditional counterintelligence or cybersecurity won't be able to do much to stop such threats. Just as TikTok could hide its intentions inside the algorithm, AI can hide its intentions. It might take years to carry out an information attack, making even statistical-based approaches to proving culpability impossible. Moreover, AI may become ubiquitously used by people and highly scaled to affect millions, if not billions, of people. Technology must be used to fight such technology.

★ ★ ★

AI may be the cause, but it is also the cure: we will need to use AI to find and root out AI-generated information threats. The IC and law enforcement are already unable to track the thousands of propagandists now operating. With millions or, indeed, billions of AI propaganda machines preying upon society, the only means to stop them and protect ourselves will be to turn to AI. We need to create counterpropaganda AIs equipped to help navigate this information hyperreality. As Churchill said to Stalin, "In wartime, truth is

so precious that she should always be attended by a bodyguard of lies." AI can act as our information bodyguard, our mind's guard.

In some ways, this AI bodyguard would look just like the AI propaganda tools we are trying to fight. It would monitor what you saw, read, and heard. It would build a model of you and continuously update that model. It would become expert at understanding how you thought and what you needed.

But it would not feed you information or filter anything. To do so would just create the same problem it would be trying to defend against. No matter how beneficial it might sound to have a "good" source of information, the good source could always end up being bad, influenced by other sources or beholden to someone or some organization with a bias.

Rather, our mind's AI bodyguard would be charged with two things. One would be to act as a collection and warning system for disinformation. It would see disinformation in the wild, perhaps matching a central database created by the government or a civilian group. Or perhaps it would note statistical anomalies, such as a surge in the amount written on a topic, and determine whether there was a threat. It would report that information to you and also to other AI bodyguards to warn others. It would also report other people's AI bodyguard warnings to you. Think of it as your personal counterintelligence officer.

The second thing our mind's bodyguard should be charged with would be to act as an AI co-pilot for truth. Its goal would be not to filter information but rather to get you to ask questions about what you were hearing or seeing. As for the philosopher Socrates, its job would be to ask questions. Perhaps it sees a lack of sources in an article you are reading and asks you about that, suggesting some additional articles to read. Or perhaps it notices a series of statistical anomalies in how several pieces of information are being presented to you on a specific topic, indicating that maybe you are under a disinformation attack, and it asks you what you think about that. Rather than feeding you answers, it might feed you questions. In such ways, we can imagine an AI that balances the need to defend against AI disinformation with its not becoming yet another vector for information control.

★ ★ ★

This is a vision of intelligence that is very personal, literally something that is inside our minds, but we usually think about intelligence as something done by kings to other kings or states to other states. Julius Caesar needed intelligence to win his wars for Rome. Popes needed to know what the Medicis were conspiring about in Florence. Queen Victoria wanted to protect her empire, as did the Habsburgs and every other nation or empire in Europe and pretty much everywhere else.

To pursue these ends, small groups of spies evolved into massive, intricate, and above all secret bureaucracies. In the United States, informal espionage in the Revolutionary War led to military intelligence units, the OSS, the CIA, and the dozen-and-a-half agencies of today. These agencies are now confederated in the Intelligence Community, part of the toward-a-whole-of-government approach from the third intelligence revolution. Intelligence in this vein has seemed like something done by agencies and governments to other agencies and governments.

The fourth intelligence revolution extends intelligence much farther. First, it spreads into the whole of nation. That includes not only government agencies but also companies, nonprofits, universities, and other groups. But the revolution does not stop there. Intelligence is breaking the boundaries of agencies and governments and even companies and reaching into society at large.

Authoritarian governments have already beaten us there by directly attacking society and citizens. Their intelligence agencies increasingly target everyday Americans—indeed, everyday people in general throughout the world—as part of their intelligence-collection and information operations. They do this because they have come to realize that in a connected, networked world, people matter. Everyday people work at companies that these authoritarian governments want to spy on and steal from; they vote, they take part in government, and they maintain views at odds with authoritarians' constructed realities. This makes everyone a potential threat. By using AI, our adversaries can take this targeting as far as directly targeting our minds, hacking us the way they hack our computers.

But worse still would be to have our own government purposefully or inadvertently use AI or other cognitive means to influence our thoughts. There is a terrible moral hazard of even the best governments falling into the trap of authoritarian thought control. With this in mind, we as citizens should be concerned and mindful of any government with the ability to change our minds.

This shift from intelligence being about leaders and governments to its being about everyone is the biggest paradigm shift of all in the fourth intelligence revolution. This is the democratization of intelligence, and it will force us not only to rethink intelligence, but also to learn to think differently about our everyday world. At its most extreme, the fourth intelligence revolution will lead us down a path where we cannot turn to intelligence agencies for protection but, instead, will need to turn to our fellow citizens. In other words, everyday people must protect themselves and fight back against this intelligence collection and cognitive warfare.

OceanofPDF.com

17

Citizen Intelligence

At 12:31 p.m. on July 17, 2014, Malaysia Airlines Flight MH17 departed from Amsterdam Airport Schiphol. It was supposed to land in Kuala Lumpur some twelve hours later, but instead, it encountered tragedy over Eastern Ukraine. At around 4:15 p.m., a Buk surface-to-air missile, capable of engaging targets at high altitudes, climbed rapidly into the sky. The Buk is a formidable weapon. It uses radar to track its target and detonates a high-explosive warhead in proximity, sending out a lethal shower of shrapnel. The missile's range and altitude capabilities made it a deadly threat, especially for a commercial passenger plane like MH17's Boeing 777, which had nothing to protect it from such an assault. The innocent passengers inside were sitting ducks. All 298 people on board died.

Over the following weeks and months, the who, what, where, and why of the puzzle came together. It turned out that MH17 was not the target per se. The passengers and crew were innocent victims caught in a long-simmering conflict that had nothing to do with them.

Between the annexation of Crimea in the winter of 2014 and the full-scale Russian incursion into Ukraine in 2022, Putin approved sending a Buk missile system to Russian separatists in the self-proclaimed Donetsk People's Republic in the eastern part of Ukraine. It was one of these missiles that killed everyone on that Malaysia Airlines flight. While the exact chain of command and decision-making process remain unclear, it seems that separatists fired the missile, but the system itself originated from Russia. An official report about the incident was eventually released, but not for over a year.

In a matter of hours after the crash, though, as confusion mounted in the press, people using a new online forum called Bellingcat began to piece together the truth. Founded earlier that same year by Eliot Higgins, a British journalist with a keen eye for detail, Bellingcat grew out of Higgins's concern about the Syrian civil war. He was specifically interested in the weapons used in the conflict and their origins. Bellingcat was initially funded by a Kickstarter campaign, which is a way to have people from across the internet chip in to fund new businesses.

He named his new organization Bellingcat after a fable, "The Mice and the Cat," in which a group of mice discusses how to protect themselves from a cat. One mouse suggests putting a bell around the cat's neck, alerting everyone to the cat's approach. However, no mouse volunteers to carry out the plan, and the threat of the cat remains. The story is an apt metaphor for Higgins's work, which intended to "bell the cat" by exposing wrongdoing and bringing those responsible to account.

The idea was that Bellingcat would provide a means for Higgins and other citizen journalists to investigate conflicts and other political and geopolitical events and share information. Their approach relied on publicly available open-source information—social media posts, satellite imagery, local news reports, financial information—to piece together the narratives of these complex events.

Malaysia Airlines Flight MH17 was a defining moment for Bellingcat. By scouring social media posts, uncovering videos showing the launch of a Buk missile system in a likely locale, and using time stamps, weather data, satellite imagery, and other information gathered from public sources, Bellingcat pinpointed the exact launch location and traced the movement of the Buk system, definitively linking the missile to a Russian military unit. As meticulous as any Scotland Yard detective, these citizen journalists pieced together the puzzle, and they did it much faster than the official investigation.

Their findings, shared publicly and with international investigators, established Bellingcat's reputation as a pioneer in open-source intelligence (OSINT) investigations, and showcased the utility and potential of such a citizen-journalist approach. Since its early days focused on Syria and the

MH17 crash, Bellingcat has been instrumental in monitoring the events of the Libyan civil war, the Tigray war in Ethiopia, the poisoning of Russian double agent Sergei Skripal, and the wars in Ukraine and Israel. More than just citizen journalism, these successes demonstrate proof of concept for citizen intelligence.

Bellingcat is not alone. The internet has opened a new pathway for everyday people to work together to investigate all sorts of events. Other online communities, like Reddit, convene armchair detectives trying to crack unsolved murders and other crimes. In subreddits like r/unresolvedmysteries, users discuss theories, share leads, and analyze evidence gleaned from sources like news articles, publicly available police reports, witness statements, and victim profiles. They comb the social media accounts of the victims, suspects, and anyone potentially connected to the case, looking for inconsistencies, alibis, or clues. Users also post what they've learned from analyzing maps and satellite imagery to make guesses about where a crime occurred or potential routes of the victim and perpetrator. These online communities have certainly contributed to solving cases, helping to identify a suspect in the brutal murder of two teenage girls in Delphi, Indiana, in 2017 and playing a part in tracking down the Boston Marathon bombers in 2013. These fanatics form a true community, and some of them enthusiastically meet at a yearly convention called CrimeCon.

Some have gone even farther than just investigating. Several groups have crowdfunded drone purchases for Ukraine. There is even a group that crowdfunded the purchase of an SAR satellite that was then used by Ukrainian forces to identify and attack Russian targets—it's called the People's Satellite. It turns out that even the acquisition department of an intelligence agency can be replicated by online communities.

Like many things we take for granted, there was once a government program that considered and then proved this possibility of citizen-led intelligence. In 2009, the Defense Advanced Research Projects Agency (DARPA), one of the premier research agencies of the Department of Defense, sponsored the DARPA Network Challenge, a contest to explore the potential of social media and online collaboration for solving real-world problems. The goal of the competition was to locate ten red balloons

moored at various public parks across the continental United States to see how quickly and effectively information could be spread and used through online networks. The first team to report the correct locations of all ten balloons won a forty-thousand-dollar prize. Given how spread out and randomized the balloons were, the only way to win was to tap into the power of the internet, using social media and online resources to connect people from all over the country to a single project with a singular goal.

In the end, the winning team, the MIT Red Balloon Challenge Team, identified all ten balloon locations in the astoundingly short time of under seven hours. This was a clear demonstration of the potential of regular people using open-source intelligence and the command, control, and communication powers of the internet to tackle an intelligence mission. The implications are far-ranging, including military operations and disaster relief, and the challenge showcased how the government could task citizens to perform intelligence work.

These citizen-driven investigations and projects have a unique set of pros and cons. On the positive side, they can tap into people anywhere in the world, leading to a truly global network of information collectors to give firsthand access to local information. For example, in 2011, a local Pakistani man in Abbottabad live-tweeted the highly secret U.S. raid that killed Osama bin Laden, showing that even the most secret operations can’t be kept secret for long. In other words, the entire world population is a potential source of intelligence. Additionally, the diversity of users brings a range of skill sets to the hunt, from experience in forensics to criminal profiling to geolocating. Some may also be highly skilled technologists, with the ability to use AI and other cutting-edge technology in an agile way that the rule-bound Intelligence Community, sitting behind classified systems, can only dream of.

On the negative side, users typically don’t have access to the full investigation details or all the physical evidence. They also are limited to open-source collection, and while they might have access to commercial satellites, they certainly don’t have access to the more capable classified satellites. Finally, with an open collective, there is always the danger of its being infiltrated by sabotage, disinformation, or other adversary

counterintelligence attacks. Ultimately, while these users are not professionals, the difference is just a matter of training, data, and tools.

The CIA and other agencies obviously have amazing analysis training programs, but the IC does not have a monopoly on intelligence training and capability. For example, it has been proven that even a modicum of very specific training can make some people better forecasters than the most highly trained intelligence analysts. In 2010, the Intelligence Advanced Research Projects Activity (IARPA), the Intelligence Community's version of DARPA, funded the Aggregative Contingent Estimation (ACE) program. Its goal was "to dramatically enhance the accuracy, precision, and timeliness of intelligence forecasts for a broad range of event types, through the development of advanced techniques that elicit, weight, and combine the judgments of many intelligence analysts." In other words, to make intelligence forecasts better using crowdsourcing. The research program set up the equivalent of the geopolitical forecasting Olympics, where teams competed to see which could best predict discrete geopolitical events.

One of the most successful teams was Good Judgment Project, which was managed by University of Pennsylvania professor Philip Tetlock. This team recruited regular people who were not geopolitical subject matter experts. The participants were given tailored training in overcoming psychological biases and using certain forecasting best practices. Tetlock's team used an algorithm to aggregate the forecasts, and the group was reportedly 30 percent better at forecasting than intelligence analysts using classified information and analysis systems.

Also, while the Intelligence Community may have a monopoly on classified systems, it's not always the case that secret data is better data. For some issues, like economic security, open-source information is better than classified information for forecasting. The sheer number of sources can be helpful, in comparison to the relatively limited number of available classified sources. Moreover, the concept of the wisdom of crowds—in which collected and averaged views may be better than any single opinion—may push the best open-source approach to the top.

At the same time, the technology available in the commercial world is sometimes more cutting-edge than what's available to the government.

Government acquisition programs take years to develop and implement new analysis systems. The tools are good, and they get the job done, but they are built upon five- or even ten-year-old technology. Meanwhile, data analytics and AI technology are improving by the week and may be implemented within weeks of their invention. OpenAI, Anthropic, and other generative AI tools are much easier to access from your cell phone than from inside the halls of the CIA. Half my job at the NGA was to figure out how to get these commercial data analytics and AI systems into the agency, and I wish I could say I was more successful.

This isn't the first time regular people have been doing intelligence. Before OSS, there was no true peacetime intelligence organization, but there were people collecting intelligence. Bill Donovan was running around Europe, from Nazi Germany to Mussolini's Italy, having conversations and taking notes and sending these notes back to President Roosevelt. Beyond his law degree, he didn't have any intelligence training, and his tools were a legal pad and a pencil.

There are also some examples of the Intelligence Community breaking the boundary into civilian life. One example is Tearline, which is used to share the intelligence mission with think tanks, universities, and other public investigators. The CIA's venture capital fund In-Q-Tel bridges the gap between the government and investors. Another example is the work of the United States Geospatial Intelligence Foundation (USGIF).

USGIF is a nonprofit formed in 2004 to promote geospatial intelligence tradecraft and develop the GEOINT community. This was around the time of the birth of the NGA; the agency was previously known as the National Imagery and Mapping Agency. More than just a change in name, the refashioning of the organization reflected the birth of the new multidisciplinary concept of GEOINT and its growth in value. General James Clapper is a legend in the world of intelligence who served for more than fifty years as an Air Force general, director of the NGA, director of the DIA, undersecretary of defense for intelligence, and the fourth director of national intelligence. When he was the NGA director, he realized that this new form of geospatial intelligence would require a new type of

cooperation with industry and academia, and so he had USGIF set up to support this partnership.

Unique to the world of intelligence, USGIF is a completely open organization made up of current and former intelligence officers, academics, businesspeople, and anyone with an interest in the space. The organization promotes GEOINT, holds educational courses on tradecraft, offers an accreditation process, and supports the development of new tradecraft. But the most important thing it does is get everyone in this field together, from undergraduate students to agency directors, to figure out how to do better GEOINT. One way they do this is through a yearly GEOINT conference, in which several thousand people get together, catch up with old friends, hear about what is going on in the field, exchange ideas, clink glasses, and create an open community around an area of intelligence. This might have been unimaginable in the Cold War days of highly secret agencies, but today, anyone can sign up.

Tearline, In-Q-Tel, and USGIF are examples of how the third intelligence revolution began to open intelligence to the public, compared to the Cold War. However, all these projects have one thing in common: the official involvement of the Intelligence Community.

The fourth intelligence revolution will go much farther in severing the direct ties with the Intelligence Community to democratize intelligence. Everyday people, citizens of our country or other friendly nations, will conduct intelligence themselves. They will do this without the government in charge or involved. Imagine something like a Bellingcat, but focused not just on investigative journalism but also on defending the American people. Just as revolutions led to democratic governments, this revolution will lead to democratized intelligence. We as citizens—and by that term, I mean our identity as members of civil society as opposed to literal citizenship, in the spirit of citizen journalism—will and must form a new type of citizen intelligence.

The benefits and capabilities of citizen intelligence have been demonstrated by activities like Bellingcat and the ACE program. Citizen intelligence can move very quickly to investigate, use open-source intelligence better than intelligence agencies, and tap into millions, if not

billions, of people in the world to chip in and help. Where citizen intelligence really shines is in countering disinformation and other areas where involvement by the Intelligence Community can be problematic due to censorship and other legal, political, and ethical concerns. Citizen intelligence is a path to monitoring and shutting down new disinformation vectors on platforms like TikTok. It puts the onus of action on the entire population and is one of the few paths that will let us avoid granting the government, especially intelligence agencies, the ability to censor.

Censorship can feel like something that never happens here, where our internet is full of every possible viewpoint, but U.S. history is rife with cases of government censorship whenever national security is intoned. The Sedition Act of 1918 forbade disloyal communications about the U.S. government. There was an Office of Censorship during World War II, which, as its name implies, censored reporting into and out of the United States. Fights over government censorship have continued through today, including over Covid-19 and TikTok. To turn to the government and allow it to censor is to turn toward authoritarianism. No one wants intelligence agencies to censor information, least of all any intelligence officer I have met. Yet we must find ways to protect our society and democracy from disinformation while also being hypervigilant about our own government's power. We require a path to securing our information and our minds that does not also give our government power over our information or our minds.

We need some form of warning and support for covert influence attempts on our society, but the Intelligence Community is incapable of providing adequate information. In 2022, the director of national intelligence created the Foreign Malign Influence Center to integrate intelligence and provide analysis on covert influence against the United States and warn the public. But the IC is so protective of sources and methods—and concerned with the appearance of politicization—that the organization is hamstrung, providing exceedingly vague warnings. For example, in the lead-up to the highly contested 2024 election, the center's October announcement noted that:

> a range of foreign actors continue to try to influence U.S. elections as we approach November. These activities include broad efforts aimed at undermining trust in U.S. democratic processes and exacerbating divisions in our society, while also seeking to shape voter preferences toward specific candidates. Our assessments about the activities and goals of Russia, Iran, and China are unchanged from earlier election security updates. On the presidential race, the IC continues to assess that Russia prefers the Former President and Iran prefers the Vice President; China is not seeking to influence the Presidential election. As we approach election day, the IC also expects foreign influence actors to continue their campaigns by calling into question the validity of the election's results after the polls close.

Such warnings are so watered down and high level that they become completely useless. There is no specific warning, nor recommendation on what to do. It is reminiscent of the red-orange-green terrorism advisory system used by the Department of Homeland Security during the height of the war on terror, categories that similarly were so diluted as to provide no useful insight.

This isn't to dismiss the efforts of those in the Foreign Malign Influence Center or other government agencies. No doubt, they all care deeply and want to help the mission. It's not their fault. The problem is how the intelligence system works. The IC must protect its sources and methods. It must remain apolitical. As a society, we want both those things to be true for our Intelligence Community. In fact, the last thing we want is to have our intelligence agencies giving away their sources and getting them killed, thereby leaving our presidents and generals blind. And we definitely do not want our intelligence agencies to become politicized.

The problem is that intelligence agencies are simply not set up for providing these types of warnings; nor should they be. From our founding as a nation, through Stimson's views on reading mail, through the creation of the OSS; through the Cold War and continuing today, we have always strived to separate foreign intelligence from domestic policing. We do not

want to create a secret police apparatus that could monitor our society using the full force of intelligence capabilities. This is a worthy and necessary approach for maintaining our fundamental freedoms. In the end, the blandness of these warnings, the lack of detail, is a feature, not a bug.

Yet we nonetheless require specific and actionable intelligence on attacks on our nation that we as citizens can use to make personal decisions. If a U.S. military unit is threatened with an attack, the commander of that unit wants actionable intelligence so he can decide how to protect his troops. The president and every other leader want the same, and deserve it. Yet when the threat is against us as a society, we are left with vague warnings.

For a long time, maybe it was okay that we as ordinary civilians didn't require this detailed intelligence, because we were not quite as directly or personally threatened. The biggest national security threats were nuclear weapons, tanks, and terrorists. These threats were dealt with by presidents and generals, whom we elected or who were appointed to protect us. Yes, it was scary that nuclear war could happen or that a terrorist could try to blow up a building, and this threatened me at a sort of theoretical level, but there was nothing I could do to deter the Soviet Union or hunt down a terrorist. But that is no longer the case. The threats are personal, and I can do something about them if given sufficient warning.

Citizen intelligence is most important because it is increasingly citizens who are the direct targets of intelligence operations. Authoritarian governments target us because we work at the companies that have intellectual property or other things they want, and we serve in roles in government that can target them. They know that our financial records, health information, and any other personal information can be used against us. But mostly, they know that in a democratic system, citizens elect their leaders, and so everyday citizens are the root of power. With this in mind, Russia, China, and other authoritarian governments have begun to monitor and try to influence democratic citizens directly. The American people are the Achilles' heel of our national security, and so we have been targeted. Our adversaries' goal is to manipulate us in order to manipulate our government. What happened in 2016 was just enough to show how

powerful such covert influence campaigns can be. Now the safety is off, and they are firing.

We are all the target of spying, and to counter it, we must all become spies. Citizens must be able to defend themselves from spying and disinformation attacks. The Intelligence Community wants to help, but it is not adequately set up to do so. We must find a means to collect and analyze our own information so we can know what is true and what is false. The question is: How does a society effectively organize and deal with citizen intelligence?

Turning to civil society is not new for the United States. Indeed, citizen community associations are at the core of what makes our country special. When the French aristocrat Alexis de Tocqueville visited the United States in 1831, he noticed something unique about it. We formed strong community associations, from towns to neighborhoods to clubs, and these associations strengthened our democracy. This feature of our culture remains to this day and has spread to every facet of life.

These community associations have included citizen self-policing, which is as old as the United States itself. Long before Russian separatists downed a Malaysian Airlines plane over Ukraine, the American colonies had formalized night watch systems, in which citizens took turns guarding against crime, vandalism, and enemy attacks. The story of Paul Revere’s Midnight Ride is, in the end, a story of a local silversmith who was concerned about British attacks and warned his fellow citizens about troop movements. The militias that fought back against those Redcoats were themselves a form of community association, led by fellow citizens. The idea didn’t end there, though. By the 1960s, neighborhood watches were cropping up across the United States, to help local police protect the community.

Now there is technology that brings community associations, and the safety derived from them, into the twenty-first century. Nextdoor is a hyperlocal app that connects people with their neighbors to share information about crime, safety hazards, and local events. Waze is a community-based traffic and navigation app that allows users to report accidents, hazards, and traffic jams in real time, helping others avoid delays

on their routes. PulsePoint is an app that allows users who are trained in CPR and the use of an automated external defibrillator (AED) to locate and assist nearby people who are experiencing cardiac emergencies. Citizen is a digital mapping platform with millions of users. It allows users to post and geolocate important information about fires, burglaries, and car crashes, ultimately creating a map of user-reported incidents that bypasses the police entirely. In essence, citizens notify other citizens of what is happening in their own neighborhoods in real time.

The social media company X is trying out citizen-driven information protection. The social network has begun using a citizen-driven counter-disinformation approach in its Community Notes feature, with which users can collaboratively add context and fact-checks to misleading posts. If these Community Notes are deemed helpful by other users, they are shared and spread. The original post stays, thus limiting censorship. This approach shows one possible path toward countering disinformation, exemplifying the democratization of intelligence. Meta followed X with a similar Community Notes feature in 2025 as a means of content moderation.

But this type of approach relies on a centralizing entity—in this case, a company. Company- and government-based solutions inherently have many of the same problems vetting information online. Centralizing any editing, fact-checking, or flagging requires someone to control information. That includes control over the tools, the data, and how the system works. This controller has an agenda and sets the goals of the enterprise. Such goals might be benign, but equally, they could be malevolent.

Companies in particular do not have the best interests of society or any person in mind, other than their shareholders. They are there to make a profit, not to ensure that society is made better, nor that national security is protected. Leaving them to be the censor of disinformation is a considerable moral hazard: they might be incentivized to allow disinformation to exist if they profit from it. Many people have argued that this is exactly what is happening on social media platforms, where the algorithms create profit from disinformation and, more generally, social strife.

Nonprofits and academia point in another direction, to disinformation watchdog groups such as the Election Integrity Network, the Center for an

Informed Public, and PolitiFact. Such groups attempt to monitor and point out disinformation online. In some cases, they might flag the content to the social media sites on which it appeared. Some groups, like PolitiFact or the more generalized fact-checking site Snopes, might check the sources and try to disprove the disinformation. Others, like the Center for an Informed Public, part of the University of Washington, try to just monitor, illustrate context, and provide alternative sources. The downside is that these monitoring organizations have been considered partisan by political groups, which has led to a series of lawsuits and political pressure for them to be shut down. As with intelligence agencies, those who monitor cannot also be political; they must be neutral and unaffiliated. While, at the same time, it is very hard to say what being political actually means, and the attacks on such groups can be politically charged themselves and driven by known political operatives. Obtaining neutrality requires that both sides of an issue be part of the process of uncovering truth and disinformation.

Wikipedia is a better model to consider, in that the Wikipedia Foundation, which manages it, does not have control over its content. Instead, the editing process is run by unpaid volunteers who adhere to a core principle of neutrality. This decentralizes the management of information. Anyone can edit almost any Wikipedia entry, which allows for a vast pool of contributors and keeps the information up-to-date. Moreover, all edits made to a Wikipedia entry are tracked and publicly visible. This allows anyone to see how the article has developed over time and to identify any potential biases or errors. If there are disagreements over the content of an entry, users can discuss them on its Talk Page. Also, there are established policies and procedures for resolving disputes. While open editing allows for a vast amount of information, Wikipedia has measures in place to ensure quality. Experienced editors can review changes, delete vandalism, and block disruptive users. Entries that don’t meet Wikipedia’s criteria for inclusion (verifiability, notability, and neutrality) can be deleted.

In some ways, Wikipedia is already a de facto citizen intelligence platform, given the way data on the site is obtained, analyzed, and referenced and the means provided for disagreement and debate. Indeed, from one perspective, Wikipedia is one of the most powerful intelligence

agencies in the world. Thousands of analysts report to millions of users and provide a version of the truth, and for many, it is the definitive source of truth.

But there is more to citizen intelligence. A citizen intelligence organization must be able to perform the entire intelligence cycle: collect new information, analyze it, report and disseminate it, receive feedback, and update tasking so that the cycle may continue.

Let’s imagine a citizen intelligence agency. It could be built like Wikipedia, as a platform acting as a clearinghouse for information and a place to collaborate. The control, ownership, and management of the agency would be decentralized, and a means to vet information would be in place, with information kept open for all to see, so that people could check sources and record changes to information. Perhaps blockchain technology would be used to ensure that all information was publicly available and tracked, remained unaltered, and was associated with the person or sensor that collected it. Citizen intelligence officers would need to be vetted as well. No doubt, bad actors would try to infiltrate this citizen agency, as they would any other. And as at any other agency, anyone and everyone would also be open for constant vetting.

The data and tools would mirror those in the IC: geospatial analysis, social network analytical tools, AI and machine learning capabilities like computer vision, and many other intelligence capabilities. The data available to users might include access to overhead imagery from commercial satellites, along with social media data, and these datasets and tools would be provided for free. Training could be provided by journalists or retired intelligence officers.

For the citizen agency to be truly decentralized, ideally the resources used to develop and run it would be donated with no strings attached or obtained by its contributors. There should be a system of governance put in place that contained checks and balances so that no individual should have control over this entity. This would also preclude single individuals from controlling the agency in general, the way Julian Assange de facto controlled WikiLeaks or Eliot Higgins de facto controls Bellingcat.

It might not be a single citizen agency; it might be many. In fact, fully decentralizing and having multiple platforms might be safer, as they could provide checks and balances on one another. One platform might be infiltrated or sabotaged or become corrupt, but another could find that out. Or perhaps the agency's various functions would be split up, with one platform concerned with analysis and another concerned with collection or different forms of collection. Again, this division could provide a check and balance and the distribution and decentralization of power.

Unlike Wikipedia, but more like a traditional intelligence agency, the civilian intelligence agency would have a mission—to protect people, communities, and society. Specifically, it would try to inform citizens of threats, such as from authoritarian surveillance or disinformation campaigns, and to work to protect against those threats. Informing people of threats would be a major part of that mission, as well as providing verified information. The agency could even go so far as to try to shut down threats by outing covert information campaigns. They might also be used to inform counter-AI propaganda machines by informing AI bodyguards in order to mitigate the issue of mind hacking. Or perhaps they might be directly involved with creating such AI bodyguards and releasing them to the public.

From that core mission, the agency's strategy, operations, and tactics could be developed over time. Like any other agency, it would determine what should be collected, how it should be collected, the types of analysis to perform, who should receive the information, and how to direct feedback to constantly improve the system. The mission and approaches would evolve over time as the threats changed. Again, unlike a normal agency, this would be done in a decentralized manner.

There could be means for liaising with the government. The CIA, the FBI, and others could share information with this group. They might warn of threats, which the group could try to address. Or they could perhaps offer challenges, like the DARPA red balloon challenge, but for real cases. The government might also share data and tools, similar to how the Tearline program has worked. Or government agencies could offer training, as has occurred in cybersecurity. Finally, the citizen agency could vet this

information like any other, being just as aware of the danger of disinformation coming from a friendly intelligence agency as from an adversarial one.

Intelligence liaison with citizens is not so outlandish. The Intelligence Community has already tried this through strategic declassification. In the lead-up to the Russian invasion of Ukraine in 2022, the National Security Council declassified and released intelligence to the public regarding Russia's military buildup, planning, and potential actions. The goal was to deter the Russians' aggression, expose their plans publicly, and rally international support for Ukraine. The Biden administration's actions made strategic declassification into a new type of intelligence weapon, one that helps inform allies and other nations, while also showing our cards to the enemy to let them know how much we knew. While informing the public is a hotly debated approach, not least because it threatens intelligence sources and methods, it does show one path toward the Intelligence Community cooperating directly with citizens.

Most important, this citizen intelligence agency would need to uphold legal, social, and ethical boundaries. It's easy to imagine how bad people, whether malicious foreign intelligence agents or just plain criminals, might try to use this platform for ill. But even people on our side could use it immorally or for their own ends. The citizen intelligence officers would need to self-patrol their ranks—ensuring that rules were followed, the system was not taken advantage of, and ethics and laws were abided by. If this sounds like a lot of responsibility to be placed in the hands of regular people at home on their computers, then I'd point out that the same responsibility was once held by a silversmith turned patriot, surveyor with bad teeth turned president, and countless other regular Americans.

Imagine if such a group existed during the IRA campaign against the 2016 U.S. presidential election, or when Chinese production companies attempted to censor American movies. Potentially, such a group could have uncovered the IRA disinformation campaign. Perhaps users might have seen the odd-looking posts and traced them back to Russian IP addresses. They could have warned the general public of the IRA's activities without politicizing them. In the case of Chinese censorship, citizen analysts could

have put the pieces together around Chinese intents and used that to mount a public campaign against the censorship. Or with TikTok, they might piece together possible covert influence patterns and warn users on that platform. A citizen intelligence agency could go much farther than the government in directly confronting these issues, without being held back by concerns over censorship, or making a diplomatic infraction, or experiencing the economic loss of being kicked out of a major market. Citizens could make decisions based upon what is best for all of us, not just a single group.

Citizen intelligence agencies would not replace traditional intelligence agencies; we definitely still need expertly trained, professional intelligence officers with classified capabilities—in the same way that we still need police officers even when we have a neighborhood watch. The world is a highly competitive place, and Russian and Chinese intelligence agencies play hardball. The United States needs to do the same using the best people, technologies, and capabilities we have. We need classified satellites to see what is hidden from us, case officers to take risks to find out what we are not supposed to know, and our own covert actions to stop threats. Indeed, there is still a role for countering information operations; while citizen intelligence may be a necessary ingredient, some covert influence will be so well hidden it requires professional intelligence officers to ferret it out or to put a halt to it once it's found.

More generally, there will always be a need for classified intelligence gathering and analysis. There is a narrative increasingly found among Washington, DC, pundits and even many professional intelligence officers that open-source intelligence is a cure-all. The idea is that there is so much commercial and other open data available that we can do all missions with it. This is overstated. By definition, if data is openly available, then the adversary has access to it, too. A commercial satellite has known capabilities and flies known orbits. Given this, a sophisticated adversary like China or Russia can hide its activities from that satellite, and the satellite will be useless. Social media or other open sources of data can be hacked, changed, or otherwise corrupted. Classified systems are classified because their capabilities are not known to the adversary. They can operate securely and overcome denial and deception by the adversary. There is

value for intelligence agencies in open-source intelligence in areas like economics, around human rights, and so forth, and we need that intelligence capability. But we need it in combination with classified capabilities that can see that last mile. This is why an open-source agency will never be the panacea some contend.

Indeed, I would argue that it is best to use a “barbell” approach in which the intelligence community invests heavily in commercial and open-source intelligence on one hand and highly exquisite, classified SAP/CAP systems on the other hand. Citizen intelligence exists on one end of the barbell, with many good benefits, but the other end of the barbell must continue to be classified.

Citizen intelligence not only helps us as a society but also helps the Intelligence Community. A citizen-led intelligence agency could work alongside professional intelligence agencies and tackle sticky issues like disinformation and censorship. Such citizen intelligence could also be very helpful to the agencies in the expanded competition areas of economic or S&T intelligence, where open-source intelligence and civilian expertise are necessary. It may also go a long way toward building trust in those who can help national security but may be skeptical of intelligence, like some scientists or human rights campaigners. Together, we can make a whole-of-society approach to national security.

Intelligence agencies will be deeply skeptical of this concept of citizen intelligence, but they shouldn’t be. For years agencies have pushed back against the idea of open-source intelligence, arguing that it is unsecure and redundant. Only recently have they begun to accept it, after seeing its value. Similarly, they will no doubt argue that citizen spies are amateurs and present serious security vulnerabilities. Perhaps they will also be concerned about the powerful tools of intelligence leaking into society and creating another power structure, similar to how a military might be concerned by the rise of militias. These are all real issues, but they also can be addressed. Amateurs can be taught and vulnerabilities mitigated in some of the ways mentioned. And, whether intelligence agencies like it or not, these tools and the idea of citizens doing intelligence are already out there. People at Bellingcat and other places do it every day. Better to tap into and guide

these people to perform mission than ignore them. Most importantly, some of the most pressing missions around information operations or S&TI cannot be done without tapping into citizens and in some cases should not only be done by government agencies if we want to protect our rights. Embracing the democratization of intelligence in the fourth intelligence revolution will be a struggle, but so were getting over our fear of peacetime intelligence in the second revolution and accepting the use of commercial technology in the third revolution. Agencies in the end can and must embrace the disruption that is citizen intelligence if they are going to succeed in the national security mission.

Ultimately, the democratization of intelligence will make our nation much more secure. An information attack or Salt Typhoon type of cyberattack may overcome our defenses or slip through the cracks of our national security system. With so many intelligence threats coming from so many adversaries and so many angles, the centralized agency construct of previous intelligence eras may never keep up. But with citizen intelligence, even if an agency missed a threat, it would still face the defenses of a nation of empowered citizens, who have tools and training to deal with surveillance or information attacks. Rather than centralizing intelligence as we once did, when, for example, naming the first peacetime agency literally the *Central* Intelligence Agency, we are now heading in the direction of decentralizing intelligence. In doing so, we all become the first and last line of defense against autocratic adversaries. Such resiliency is one of the key features and goals of the fourth intelligence revolution. This may be our best hope in combating the global panopticon intelligence mission of the CCP while also protecting ourselves against the threat of our own intelligence agencies' overreach.

Intelligence is something we should all be responsible for and play a role in, just as we are all responsible for upholding laws and reporting crimes. If you see an accident on the side of the road, you have a moral duty to report it. There cannot be police everywhere all the time. We must help our fellow citizens, indeed, fellow humans. It's the same with voting and performing public service. We have a duty to do so. It is part of being a citizen in a democracy. We all must play a role in the upkeep of the

democracy. Similarly, we should all play a role in intelligence to protect ourselves, our families, our fellow citizens, and our nation. We might even go so far as to say that citizen intelligence provides a further check and balance on government, similar to the right to bear arms or to freedom of speech and the press. It is, in that sense, a right and a responsibility.

Citizen intelligence is the most radical part of the fourth intelligence revolution. It requires us to stop thinking about intelligence in the antiquated way we still do today. The concept of a professional, government-controlled and -staffed agency as the only way to protect citizens is a construct of previous intelligence eras. There are other ways for us to protect ourselves now. Geopolitics and technology have driven us to a point where intelligence is part of nearly all aspects of life and society. When everything is securitized, everything is in the game of intelligence. Intelligence agencies as we think of them are not set up well to handle all these threat vectors. Citizen intelligence provides one way out of the morass, and it does so by democratizing intelligence.

There is a quote often attributed to the communist revolutionary Leon Trotsky: “You may not be interested in war, but war is interested in you.” The same is true of intelligence today. You may not be interested in intelligence, but intelligence is deeply interested in you. We are all being spied on, whether we like it or not, and we are all becoming spies, whether we like it or not. This goes beyond how we conduct and think of intelligence. A world of manipulative foreign powers and ubiquitous AI is forcing us to rethink information in general. Things are going so far that we are entering a world in which the line between truth and falsehood is blurring, and in that world, learning to think like an intelligence officer is our only hope. This final aspect of the fourth intelligence revolution concerns not the democratization of intelligence but its personalization.

OceanofPDF.com

18

Philosopher Spy

The Martians sent for samples of sand from the beach. With D-Day on the horizon, the British required intelligence on the French coast for the Allied invasion. The invasion commanders needed to know everything, from whether the sand could support tanks to where the gun emplacements were. Using aerial imagery, ULTRA intercepts, French Resistance reporting, and messages passed via carrier pigeon, “the Martians,” the part of the British military officially known as the Advanced Intelligence Section, produced all this intelligence and more. They went so far as to publish a sort of travel guide for the invading Allied army, which provided maps of the towns in the area, descriptions of the populations and civil authorities, information on everything from hospitals to post offices to any other information military officers would need to navigate from the heavily defended coastal fortifications to the heart of occupied France.

Thousands of Allied soldiers’ lives were saved by the Martians’ important and timely intelligence. Landing over a hundred thousand men on the coast of Normandy was, and still is, one of the greatest and most complex invasions in history, and it took a colossal amount of detailed intelligence to achieve. The success of the Martians is a demonstration of just how powerful intelligence can be.

The Martians were led with inspiration and tenacity by the austere professor of philosophy J. L. Austin. Austin studied philosophy and ancient history at Oxford, where he later became a fellow at All Souls College and lectured on Aristotle and the German philosopher Leibniz. Not exactly the background of your typical spymaster. With the war in full swing, Austin

reported to MI14 (the office in British military intelligence dedicated to Germany) as an intelligence officer. As it turned out, this man, who was described as being like a schoolmaster, was very good at intelligence, noticing details, finding insights, and revealing secrets that others could not see. He eventually commanded with aplomb the several hundred men he nicknamed the Martians. After the war, he returned to philosophy and went on to become one of the most important philosophers of his day, being very influential in the esoteric analytical philosophy area known as ordinary language philosophy.

This dichotomy is something I can appreciate, having also studied philosophy as an undergraduate and, later, become an intelligence officer. In a sense, life is about finding out secrets. Some of those secrets are of the universe. How does everything work? How are we supposed to live our lives? But finding secrets can be much more literal. If you are curious, you want to know everything, including especially what you are not supposed to know. What is Vladimir Putin really thinking? What is that Chinese satellite really up to? That is the life of the intelligence officer. In a way, there is comfort in this search. For a world that is so unexplainable, to be able to find some answers, however obscure, gives one back a sense of control.

Philosophy and espionage may seem to be strange bedfellows, but in fact they tackle the very same subject: truth. Whether or not most intelligence agencies actively engage with questions of epistemology (i.e., the study of knowledge), these questions represent the core of intelligence. What is true? How do I know it’s true? Errors, skepticism, and the innate difficulty of understanding how the universe works are the focus of philosophers. Lies, deceit, and disinformation are the stuff of spies. Both groups are innately skeptical but, nonetheless, optimistic that one day they can find the truth.

Philosophy as a profession might have started with the Ancient Greeks, but people were seeking truth long before that. For thousands of years, shamans, priests, and related classes attempted to answer questions not only about the meaning of life, but also about whether what we saw in the world was true or not. They might have attributed unexplained phenomena to evil trickster gods or to some feature of a cosmology myth. By the time

Anaximander and Socrates came around 2,500 years ago, we began asking questions about how the world works and addressing the problem of skepticism through the lens of reason and philosophy, literally, the “love of wisdom.”

The search for truth through espionage is equally as old. It is not hard to imagine that during tribal raids for cattle or conflicts over fertile land, the people involved sent spies to see what was behind enemy lines, what morale was like, and maybe to spread a few demoralizing rumors while there. Similarly, they might have been concerned that the enemy was doing the same and tried to catch such spies or to nip any rumors in the bud with their own truth. By the time the Bible was finished, it was already an old story that “Joshua son of Nun secretly sent two spies from Shittim. ‘Go, look over the land,’ he said, ‘especially Jericho.’”

As we come to tackle today’s world of AI- and disinformation-influenced doubt, we can learn many lessons from both philosophers and spies on how to deal with questions of truth. Thousands of years of seeking truth have taught these groups many lessons. And we need their help more than ever, because the battle over truth is becoming more confusing and more important than ever.

Disinformation and deception, too, are nothing new. Lying is as old as, or older than, humanity and even extends beyond it. In a competition for food, chimpanzees will use deceit to hide their actions. Plenty of animals play dead to avoid predators. People not only lie, but we have *evolved* to lie and, just as important, to detect lies. It’s not hard to imagine hunter-gatherers trying to figure out if another tribe really wanted to trade or was just using trade as a ruse to steal from or attack them. Governments and laws became a means to keep us honest. Seen through a certain lens, human society is built around lies, or at least half-truths.

As society has progressed, we have produced both more information and more lies, making it harder and harder to find the truth. Initially, information was spread by word of mouth, then by stone tablets and papyrus scrolls, and eventually by hand-transcribed books. Mass-produced printed books after Gutenberg were the start of the industrialization of information. Now books and pamphlets could be produced by the thousands

for relatively little money, instead of needing to be painstakingly transcribed. With mass printing, anyone could much more cheaply print and distribute anything they wanted, which might include truths but also lies and misinformation.

Centuries later, cheap, universally available newspapers again changed the game. A single newspaper baron, William Randolph Hearst, contributed to starting the Spanish-American War of 1898 with a disinformation campaign around the activities of Cuba, Spain, and ultimately the infamous sinking of the USS *Maine*. Radio was later used effectively by both fascists and democracies in World War II. Television doubled down on the opportunities for disinformation and made it harder to distinguish fact from falsehood, given that seeing is believing.

The internet changed this model because it allowed anyone to broadcast, leading to more information spread more quickly and to more lies. The internet meant people could now share information directly with anyone anywhere and in a decentralized fashion. Social media sites in particular meant that anyone could produce and disseminate information. While people had always been able to inform and misinform one another, the internet allowed them to do it globally and without recourse. Now anyone can create their own information and version of the truth that can seem believable to some groups of people.

AI has accelerated the proliferation of information and lies to a point that is now overwhelming. It makes it much easier, faster, and cheaper to make convincing lies. Making a persuasive fake video or fake audio was once a difficult and expensive process. Stalin and Mao had specialists do it for them. The generative AI system Midjourney, the text-to-image model DALL-E, the text-to-video model Sora, and similar technologies make it as easy as typing in a command. AI also works at scale. All those fakes can be made and multiplied infinitely. If you want to see this, just google pictures of “Pope in a puffer jacket,” “Donald Trump being arrested,” or similar, and you will see not only some convincing but utterly fake pictures, but thousands of them. Finally, AI not only spreads information, but also will be used to convince you as an individual, with laser-like precision, by hacking your mind.

Indeed, AI is taking over online information so swiftly that we are creating a counterfeit world of information within our real world. In the 1980s, French philosopher Jean Baudrillard wrote an eerily prescient book called *Simulacra and Simulation* that predicted exactly this turn. He theorized that the world is made up of simulacra, copies of things that no longer exist or never existed, and that we are now essentially living in a simulation of reality. Sharp-eyed viewers might have caught a copy of this book depicted in the 1999 sci-fi movie *The Matrix*. In college in the 1990s, I questioned that Baudrillardian reality. But today, I believe it is coming true. The internet is increasingly made up of information simulacra, and we are moving in a direction in which the internet is a simulation of reality, a closed loop where objective truth has no chance to enter. It's quite possible that AI will make so much data on the internet that there will be no new, raw data on which to train, and machines will be training on the data already made by other AI systems. Even for AI, the world's proliferating simulacra are a threat.

Into this technologically induced information-disinformation evolution comes the admixture of authoritarian governments that are systematically trying to undermine and confuse information and truth. The Chinese, Russian, Iranian, and other adversarial governments all have nefarious information operation campaigns intended to sow discord in the U.S. population. They've looked at this history of informational complexity and technological wonder just as we have. But instead of seeking ways to find truth in it, they have attempted to turn it to their own purposes.

The goal of totalitarian societies is not just to undermine any particular belief, but to undermine truth altogether. At first they tried to control truth. Famously, George Orwell wrote in his novel *1984*, "Whatever the Party holds to be the truth, is truth. It is impossible to see reality except by looking through the eyes of the Party." Dictators from Stalin and Mao to Putin and Xi have attempted the same. But the decentralized internet makes controlling truth difficult. Instead, our adversaries aim to create so much disinformation that we don't believe anything and lose our bearings on what is true, like a gymnast getting the twisties, no longer able to tell up from down after so much spinning.

When truth is unmoored and all is relative, anything can potentially be true, and we descend into danger. Consider Flat Earthers, the people who insist the Earth is flat. The danger of the flat Earth idea is that it anchors our view of what might be legitimate discourse. You might say it's easy to dismiss Flat Earthers as crazy. We've known for millennia that the Earth is round. But just by engaging with them, you've already anchored the conversation to the idea that literally anything could be true or false and that it's legitimate for people to raise "evidence," as faulty as it may be, to support any belief they want. Truth in this world starts to break down and become relative. So when something more believable but equally wrong—such as the idea that Ukraine under President Zelenskyy is controlled by Nazis or that the Covid-19 virus was bioengineered and spread by the U.S. Army—is posited, it seems *relatively* more believable.

Taken together, the internet, AI, and adversaries have combined into what I call the epistemological storm, a state in which the establishment of a truth or falsehood is made to seem relative, regardless of evidence. Anything can be made to look true or false, and misinformation and disinformation can be thousands of times the scale of true information. What is more or less true can be completely distorted, making it very hard for you to get your bearings. At the same time, the internet and other information channels are flooded with so much misinformation and disinformation that any truth can be completely overwhelmed. This epistemological storm is partially driven by the open microphone of social media, partially by the growing problem of the AI-driven simulacra, and partially by active adversary attempts to undermine the functioning of truth in our society. Like all storms, we naturally try to take shelter from this one.

Our defense mechanism in such a state is to withdraw into cynical skepticism. It's an understandable reaction that when you see enough lies and mistruths somewhere, you come to doubt everything you see there. In an interview with the *Economist*, President Biden's 2020 campaign chief technology officer, Jacky Chang, said that "most voters tend to view all messages about politics as spam, whether they encounter them through television advertising, robocalls, websites or social media." Because of this, she doubted that AI would have a big impact on elections, even if it was

producing much slicker and more targeted appeals. It's weird to think that spam prepared us to distrust AI, but it makes sense. It's not just political truths that raise our eyebrows. Increasingly, people are skeptical of scientific, social, and all other forms of information. It's almost like our information immune system has been triggered too many times by exposure to lies, and now any whiff of a falsehood leads us to full-blown skepticism.

However, just as an autoimmune disease can be dangerous for a person, cynical skepticism is dangerous for our society. Humanity cannot progress without trust. It is hard, if not impossible, for a democracy to work if people can't debate from a place where they believe in the idea of some objective truth. Worse still, people may become so untrusting that they no longer believe in the social good of law enforcement or the role of government-produced money. Right now, a small minority of the U.S. population refuses to believe in the validity of the government as sovereign. These people are very dangerous, and they can and do sometimes shoot police officers, arguing that they are outside any rule of law represented by the police. Some people exchange gold and silver instead of dollars. With enough people thinking this way, the state and even the economy could break down, and society would begin to resemble anarchy. Again, this breakdown of trust plays into the design of autocratic adversaries, who would love nothing more than the disintegration of the U.S. social and political systems.

Even if things don't go so far as that dystopian state, distrust will still harm all our lives. Just waking up every day and having to wonder whether something you read online is real or not is exasperating and inefficient. You need information to live, do work, and have relationships. Consider our professional lives. Can someone trust a scientific article while working at a research lab? Can an investor trust due diligence information? Can journalists trust what they hear, see, or read when writing an article?

The proliferation of distrust is a major problem for the world of national security. Being wrong is one thing, as the United States was when we invaded Iraq under the false belief in that country's possession of weapons of mass destruction. That is terrible enough. But it would be much more nefarious if there were a systematic breakdown in which all

information could be right or wrong without reference to reality. We're entering a world in which the military might systematically prepare for wars in the wrong places, leaving the door open to attacks in others; or where the Chinese Communist Party might attack the American public with strategic and targeted propaganda, but instead, we decide not to believe the attack is occurring. This is the sort of future we can expect. In fact, it's a present we're already experiencing in some ways.

This dissolution of truth is the ultimate problem to which the fourth intelligence revolution must respond. Imagine a world in which an intelligence agency brought a president a report that its analysts verified as true based on empirical evidence, but that the president did not believe, distrusting the agency's version of truth. Or, even worse, what if different analysts have different versions of the truth and cannot come up with a definitive view. Just as truth breaks down in society, so it does in intelligence.

The Enlightenment version of truth has a means of dealing with this: through critical thinking and debate. People with different views fight it out, and the best view, defined as the one with the most evidence and logic, wins. This, however, doesn't work when someone rejects the concept of there being an obtainable truth a priori (i.e., before it begins). Now anyone can define any truth they want. This means that not only can the president define something as true or false, but so can anyone in the administration or even the public, and there won't be a means of convincing them or of their convincing you, other than by faith in that person. And even that person's truth may come to be seen as false by their true believers.

This attack on truth is a generational problem, as it affects children even more than adults. Maybe today you feel you have enough basis in truth from a long life to get by, but that is not the case for the next generation. Children have no basis by which to understand the world until they are taught. But what do you teach them if you aren't sure what's real? Or what if they are taught false information through the internet or a predatory AI? It's no accident that Mao turned to a younger generation for his Cultural Revolution—children and students had no referential experience in the world before his Communist Revolution and could be

taught to believe anything he wanted. The consequences were disastrous. Millions died, and the aftereffects are still being felt in China decades later. Authoritarian governments like China know that children can be manipulated, and this can be used to change generations. This is why the Chinese specifically target young people with sites like TikTok. They are targeting not just today's leaders and intelligence officers, but also tomorrow's. As the epistemological storm spreads, whole generations of U.S. citizens, leaders, and intelligence officers will be swept up in the deluge.

Navigating Scylla and Charybdis in the fourth intelligence revolution is about not submitting to the chaos of the epistemological storm while also not falling under autocratic information control. Just as China parasitically used our surveillance system against us with Salt Typhoon, our adversaries are using our freedom of information against us, creating a threat out of our own system. But there is only so much that intelligence agencies can do to protect us from the epistemological storm. To do too much would be to just create yet another voice in the maelstrom. Or, worse, government intervention could create a bigger threat, through building our own autocratic system of information control. Instead, we must learn to live with and navigate this storm on our own, and in that way we will become more resilient as individual citizens and as a nation.

While there is no easy solution for living in an epistemological storm, there are some lessons that we can learn from philosophers and spies, two groups of people who are trained to think about and deal with the complexity of truth and doubt. They can be our lighthouses in the storm.

Intelligence officers are quite literally trained by governments not to trust, yet to still operate and get the job done. They must deal with the ambiguity of trying to figure out what is true when there is never perfect information, when they never have as much information as they want, and when sometimes there are errors in the information they do have. But on top of that, intelligence officers are up against adversaries who are explicitly trying to deceive, limit access to information, create disinformation, and generally disrupt truth. This background illustrates the major difference between the mission of the philosopher and that of the

intelligence officer: for one, the information is obscured by the universe; for the other, it is obscured by the adversary.

James Jesus Angleton, the paranoid head of counterintelligence at the CIA from 1954 to 1974, spoke of the wilderness of mirrors, in which deception, double agents, and information operations sowed confusion. He and other spies throughout history developed a series of tools and approaches to dealing with this confusion. These tools are applicable to our epistemological storm. One guide they have used is the so-called Moscow Rules, an unofficial set of guidelines for operating in a paranoid, counterintelligence-filled Moscow during the Cold War. The first rule is simple: Assume nothing. The second: Trust your gut. Being suspicious can be good, including about your own assumptions. What might seem normal in one place and so be assumed (such as that most information you see coming from a friend is real) may not be true. At the same time, we have evolved to be good at lie detection, and oftentimes, it is an intuitive, gut sense that tells us. If something seems off to you, it probably is.

A rule we might add is to never fully trust any single piece of information on its own. Any piece of information that comes to you may be compromised, and so you should question it. One way to deal with this is through triangulation. Maybe you have a source tell you something. Now try to find an unrelated source to see if you come up with the same result. Ideally, these sources should be not only unrelated, but also completely different types of intelligence. For example, maybe you get a piece of information from a human source and another from a satellite image. Even better, get more than two pieces of information.

A corollary to this is to know and continually test your sources. A source may be extremely trustworthy based on your experience, but on any day, that source could become compromised. This leads intelligence officers to operationally test—or “ops-test”—sources of information. We might have a HUMINT source collect information that we already know and see if it matches. Or we might recalibrate the sensor on a system using another sensor.

Continuously look for new information to update your understanding. The world changes as history marches on, and we make new discoveries

that change the truth. Perhaps a foreign leader is your ally one day, but he easily could become your enemy the next. It's the job of the intelligence analyst to continually reassess conclusions based upon new information. Just because you know something at one minute doesn't mean it's true the next minute. In essence, you need to build a mental model of what you think is true in the world and continue to update that model over time.

These are very practical and useful approaches in our daily lives. When you are reading news on the internet, you can look for multiple sources, not just within the same circle of ownership or with a similar bias. Something you see in the *Wall Street Journal* (or whatever your favorite news source is), a source seemingly trustworthy to you, could still be wrong. But if you see it in the *Journal*, on the BBC, in the *New York Times*, on Newsmax, and in the *South China Morning Post*, it is much more likely to be true, because these organizations have different owners and biases. Even if you do find a source you trust, continue to operationally test it. Maybe there is a journalist you like; still, every now and again, you should go check their information. Perhaps even do some of your own firsthand research, such as visiting the places they mention or looking at live streams from them. Finally, keep an open mind and update your mental model. You can start by making your model a little more explicit, perhaps even writing down what you believe and why you believe it, and then continue to check in on this reasoning as new information becomes available. Explicitly ask yourself whether your assumptions are still correct.

Philosophers are perhaps the only people more skeptical as a group than intelligence officers. Just how skeptical are we talking? Well, according to them, maybe my whole world has been constructed by an evil demon, as Descartes says, and nothing at all around me is real. Or perhaps, as in American philosopher Hilary Putnam's modern version, we may just be "a brain in a vat" and everything around us is a generated hallucination. In such a situation, nothing might be real, other than maybe that there is a "me" to ask that question—and even that can be questioned. The ideas get even more esoteric from there. Distilling thousands of years of lessons around skepticism and the broader area of epistemology (the study of knowledge) is tough, but there are a few lessons we can take away.

Question everything, including yourself. It's not only about whether you believe something. Ask why you believe it or don't. Perhaps it is because you have an underlying bias to believe or disbelieve certain things. Maybe you want something to be true (or false). Our experiences have conditioned us in certain ways, and it is worth examining how, because that may cause a bias. Such internal biases can skew not only a single piece of information we receive, but all information. These lessons go back to the beginning of philosophy and the inscription on the ancient Temple of Apollo in Delphi: "Know thyself."

At a practical level, we should be skeptical, including about our own biases. When you see information online or are told something, even by a friend, you should always question it. Who was the source of the information? How did they learn that information? Do I believe this particular piece of information in this article because it is my social or political bias? Or am I really questioning it? This goes for our own government, too. You might be a patriot; perhaps you have even served in the military or in intelligence, but that does not mean you should accept everything you hear. Remember, in the end, the sources of intelligence presented by Colin Powell to the UN Security Council on Iraq's weapons of mass destruction were wrong, and therefore, he and the Bush administration as a whole were wrong. No one can let their loyalty or patriotism get in the way of the pursuit of truth. It's actually your patriotic duty to question. The same goes for anything you believe in and support.

At the same time, we must have something to stand on. Descartes ultimately said that even if the demon was holding him hostage and hallucinating his world, there was still a self. Famously, he stated, "Cogito, ergo sum," or "I think, therefore I am." From there, he could build a world of true things. We don't all have to go to such lengths every day. But maybe there are some basic facts you do believe or sources you can trust. Maybe it's what you see with your own eyes.

A practical way to assess what to stand on as true is to consider how hard it is to change. Take an example from traditional espionage. Say a would-be source in Soviet Moscow meets an MI6 case officer but does not trust that the case officer is actually with MI6 and the British government.

The case officer could, after all, be falsely pretending to be with MI6 and is actually a KGB officer testing the would-be source's loyalty and looking to put him in prison. Thus, the would-be source might require proof that this case officer was really with MI6 by doing something only a real MI6 officer could do. Just saying that you work for MI6 is not enough; anyone could say anything they wanted and be lying. A way around this is to demonstrate trust by doing something very hard to do, such as to place a visible *X* or other signal inside the window at the British embassy. It would be very difficult for the KGB to do that but straightforward for an MI6 case officer associated with the British embassy. Though this does not provide complete trust, because in theory it is possible the KGB infiltrated the British embassy and made the *X*, it is more believable. This is an example of what in espionage is called presenting bona fides. The harder the bona fides are to demonstrate, the more believable they are.

Similarly, it's very easy to post an article on a random social media site saying that the president said something, so it is not very believable. It is harder to post on the official White House website, so that might be more believable, but still not full proof, as the site could be hacked. However, to have something said in a public speech in front of the White House by an official press secretary and filmed by multiple networks would be very hard to fake. This gets to the relative nature of truth, with some things being more or less trusted due to their difficulty to counterfeit. It also gets at how we can see truth as something that is based on practicality. We all, as with the would-be source in Soviet Moscow, might never fully know that something is true at a deep, epistemological level, but we can practically believe that some things are pretty much true because they would be so hard to fake.

Along these lines, there is one uniquely American school of philosophy that may be of help. It's called pragmatism. Greatly simplified, one of pragmatism's principles is that there may not be any real foundation for truth. But beliefs about the world are evolutionarily necessary to survive, and you can still use beliefs to survive, even if they are not necessarily true. A major philosopher associated with pragmatism, William James, referenced the idea of "truth's cash value." If that's not the ultimate

American philosophical phrase, then I don't know what is! The philosopher Richard Rorty went so far as to argue that pragmatism is fundamentally antiauthoritarian, not just politically, but with regard to any form of authority. While this may not be the rock-solid grounding some would want for truth, it does give us somewhere to start. The usefulness of truth can be measured and provide a means to carry on with life through this "truth's" usefulness in doing practical things, whether that be science, commerce, governance, or security. And we need something to stand on if we want to continue to move forward in our increasingly confusing world.

The critical lesson to be applied to today's reality of adversary-led, AI-generated disinformation is that we can no longer be passive; we must be active consumers of information. It is about actively seeking, assessing, and reevaluating truth at all times. This is a mind-set change. Television was a one-way street; information was broadcast to us. The internet has been a two-way street; we are broadcast to and can broadcast back out. The next AI-driven phase of information will be about actively interacting with information: taking it in, considering it, changing it, finding what is useful and true, and always questioning it. Being an active consumer of information is a lifelong process. Our mental models of the world must be continually updated, our understanding of our sources and of ourselves must be continually checked, and even the underlying foundation of our worldview must be constantly questioned.

The ultimate irony is that the biggest thing spies can teach us is not to doubt but to trust. Turning to cynical skepticism and trusting nothing is a first-order defense against a world in which information is continuously manipulated. But ultimately, we need to trust something if we are to function as individuals and a society. Intelligence officers must eventually find something to trust, to some degree, because they must do their job, which is to provide decision makers with useful information. We can't just exist in a state of doubt; at some point, a decision must get made, whether that is to believe a newspaper article or to send soldiers onto the battlefield. The key is understanding how to gain that trust.

The tools of intelligence and counterintelligence can and should be taught to everyone. Many of us experience this every day, when our work

tells us not to open phishing emails or to regularly change our passwords, for example. We should take steps to go beyond training for common cyberattacks and, instead, consider the totality of the intelligence ecosystem we all live and work in today. These lessons should include triangulating information, continuously monitoring and testing sources, updating our mental models, being skeptical of information, and in general actively interacting with what we see and hear, especially on the internet. We seem to be more focused on securing our computers than securing our own minds, and that must change.

The first step is to change the lens through which you look at the world. By knowing how our adversaries work and their means of collecting our information or manipulating us, you will be able to see through their deception and understand what is really going on. This is something I hope this book has illustrated. Now once you see it, you can defend yourself. There is a saying in intelligence: “You can’t case-officer a case officer.” Once someone is trained to do something, they will see the trick from a mile off and be inoculated. We all need to be thinking all the time about information, trust, and verification. Once you start to think this way, once you see the world through this lens, you will be able to protect yourself.

These are lessons for all of us, and I would go so far as to say that we must prepare our children to encounter information that has been purposely and maliciously manipulated. It is not enough to teach someone that information might be wrong. They need to be taught that there are those who purposely try to manipulate them, those like Descartes’s demon, but real, and with large budgets for intelligence and covert action. If it seems crazy to teach a child that China and Russia are trying to manipulate them, remember that we also taught them to hide under desks in the event of nuclear war, and we currently teach them active shooter drills. Children know there are bad people out there. Generation Alpha can be, will be, at the forefront of a generational change, a shift in mind-set and approach when it comes to identifying what is true and what is not. They are part of an ideological battle, not unlike the anti-communist one their grandparents fought and the fascist one their great-grandparents fought, but this one is even more complex and confusing.

More generally, we can prepare children for the epistemological storm, and one place to start is by teaching philosophy in school from a young age. Children are natural philosophers and already question everything. That should be promoted. If you have ever had an eight-year-old in your life, you know what it is to have a Socratic dialogue. Everything is on the table—from why the sky is blue to why we say “thank you” when receiving a gift. There are real lessons to be learned about how knowledge works and how to walk the line of skepticism. The biggest lesson of all is to teach them to not necessarily trust their teachers. Many of us were taught, for example, that Columbus discovered America. We were then surprised to learn later in life that Vikings came to America well before Columbus. More fundamentally, the whole idea of Columbus (or the Vikings) “discovering” America is just something seen from the perspective of Europeans, rather than from that of the millions of people who already lived in America and had been there for ten or twenty thousand years. Questioning teachers and “accepted” knowledge is not only okay but important to do. The point is that children are naturally active learners, and this process of active learning, useful skepticism, and dialogue with truth are valuable survival tools in the epistemological storm.

Children should be taught to strike a balance between learning and accepting truth and questioning and thinking for themselves, and that is a lesson of both philosophy and intelligence. Even the educational system may become a battleground of cognitive warfare, as with Chinese education technologies, for example. Certainly, the social media environment already presents an information front line, and much of what children, especially teenagers, learn is to be found on social media. Thinking for themselves and having the tools of the philosopher help. But so does having the caution of a spy, wondering not only whether something is true, but also whether it might be part of an adversary’s assault. These are survival tools in an information world filled with information predators, just as one day, long ago, recognizing the tracks of a wolf might have been a survival tool to be taught to children.

Though the challenges of a world in which adversaries try to undermine our society through manipulating truth are real, there is hope.

We can learn how to spot and confront the manipulation of information. There are lessons that can be taught to children to raise a more resilient generation. We can come to a point at which we do not just rely on shadowy government agents to protect us, but instead we are also able to protect ourselves. This is the ultimate nightmare for authoritarians. They want to prey on unsuspecting populations, but we do not have to be unsuspecting. It is much harder for them to harm us when each of us can see right through their tricks and maintain our own personal bodyguard of truth. In the end, while it is true that there are those trying to harm us, we can defend ourselves. We can be resilient and, thereby, our nation can become resilient.

OceanofPDF.com

19

Intelligence 4.0

The fabled CIA Director Allen Dulles was responsible for building what is today known as the Original Headquarters Building in Langley, Virginia. When it opened, he had a quotation etched into the lobby, which still greets visitors to this day: “And Ye Shall Know the Truth and the Truth Shall Make You Free—John 8:32.”

The question of what is true has always been at the heart of intelligence. For Dulles’s CIA, operating amid the Cold War, the KGB presented an arcane maze of espionage and intrigue, Angleton’s wilderness of mirrors. The CIA needed to navigate that maze, find the truth, and hide its own truths. Since then, it has gotten only more complicated to know the truth. Today, social media distorts and obscures, multiple intelligence agencies manipulate and obfuscate, and, increasingly, artificial intelligence creates information and so-called truth from thin air. Yet today, the question of truth is even more critical. Without a firm foundation in what is real, it becomes easy to believe that down is up or, worse, wrong is right.

In the meantime, threats grow in number and sophistication every day. China has hypersonic missiles that could evade all our current defenses. Russian operatives blanket the world in disinformation and are unafraid to assassinate their enemies or to invade neighbors. North Korea builds nuclear weapons and ICBMs. Terrorists continue to plot the slaughter of innocents. Anyone can develop viruses that might lead to global pandemics even more catastrophic than Covid-19. And nefarious actors across the world are programming AIs with the potential to threaten freedoms.

Defending against these threats is as much the lifelong duty of intelligence officers today as it was seven decades ago.

But as terrifying as all this sounds, we can stay ahead of these threats.

The United States is still by far the most powerful nation in the world in terms of military and economic might. More than two million people serve in our military, and nearly another million work with the military as civilians. Moreover, these people are extremely well trained, and most of the leadership has years, if not decades, of experience commanding in wartime. Eleven U.S. aircraft carriers patrol the world's oceans. We spend more on our military than the next ten countries combined, including China. For all the talk of China surpassing us economically, the U.S. economy produces trillions more than China's. The United States leads in nearly every industry necessary for power, from being the largest oil producer in the world to creating the most cutting-edge AI. These are real markers of hard power that should not be dismissed.

U.S. soft power remains equally strong. NATO and Five Eyes are decades-old alliances. We have fought multiple wars shoulder to shoulder with allies. The United States retains powerful positions in the United Nations, International Monetary Fund, and the World Bank, among multiple other international institutions. American culture continues to set the standard for billions. The draw of the American dream brings in legions of immigrants every day who look for a better life.

More than just having more money or more guns, our true strength lies in our liberal democratic system. For all its frustrations, liberal democracy is better for humanity and will inevitably defeat autocratic enemies. The key lies in the values underlying our system. Trust in our fellow citizens and leaders provides a stability autocracies can never have. While it can at times seem like trust is diminishing, it is nonetheless a hundred times stronger in democracies than in autocratic societies, where dictators spend most of their time trying to control their citizens through coercion. Democratic elections allow societies to vote out parties that pursue bad policies. Meanwhile, poor-performing but enmeshed dictators can run countries into the ground. Indeed, it is the rough-and-tumble process of constant elections that guarantees resiliency, where competition pushes performance, versus the

fragility of autocratic systems, which are static. Basic rights and the rule of law undergird democracies with a stability and predictability lacking in autocratic countries. There are real benefits to this liberal democratic way of doing things, from promoting a thriving creative economy to attracting the best and brightest from the rest of the world.

Some have argued that these liberal democratic values are an impediment to national security, but it's the opposite. Having a nation controlled by single lifelong dictators like Xi or Putin might give the impression of stability. Or removing personal rights and freedoms might appear to give autocratic systems an immediate tactical advantage in intelligence. But this is not true. There is no check on the power of an autocrat like Xi or Putin that might help to halt his bad decisions, as elections do. Xi's and Putin's people do not trust them, and Xi and Putin do not trust their people, meaning decisions about rule and governance are made out of fear. Putin's people could not communicate to him how bad the invasion of Ukraine is, because of their fear. Xi spends most of his time and most of his national security budget on controlling his own people, obsessively trying to maintain power. A nominal gain in tactical advantage in data collection by sacrificing personal privacy and basic freedoms is hardly worth the near-complete breakdown of social trust, not only domestically but also internationally. Hence, I disagree: liberal democratic ideals are not impediments to national security; they are the foundations of it.

Most important, the United States will succeed because, unlike in autocratic nations, we are all in this together. We can all be part of the solution. Putin and Xi would never trust their people to be part of their intelligence apparatus. Their intelligence agencies exist first and foremost to ensure that their regimes are protected from their own people. We are an open society, and they are closed societies; and that goes for the way they and we handle and conduct intelligence.

While we can and should be hopeful, we must recognize we are nevertheless in the middle of a fight over who has the competitive advantage in a changing world. New technologies and new power dynamics have upended our traditional sources of power. We cannot rest on our

laurels. This new competition requires us to ignore our traditional sources of power and reinvent ourselves, even when it goes against our intuition and instincts.

In today's gathering storm, our adversaries have turned to asymmetric approaches to combat the United States and the West. China, Russia, Iran, North Korea, and terrorist groups all know that they cannot confront us directly in our areas of strength. As with the insurgents of history, they are instead confronting us in areas where we are weak. Today, economics, science and technology, natural disasters, human security, biological attacks, and even deep space are major parts of competition because they are all areas in which we are not set up to compete well. Our intelligence agencies are classified and do not work well with open-source information, nor where they overlap with domestic issues and American citizens. The scope of intelligence has expanded into areas for which we are deeply uncomfortable.

In this greatest asymmetry of all, authoritarian governments have realized that the best way to target our nation is to target our people. This means we are all targets of intelligence, as our adversaries are collecting our information and covertly influencing our thoughts. Social media and global ubiquitous surveillance technologies give those adversaries the vectors for these attacks. The adversaries prey upon the soft underbelly of our nation, taking advantage of the very rules and values that underlie our society, from freedom of speech to democratic elections.

Artificial intelligence and autonomy technologies are powerful accelerants to the changing landscape of intelligence. They are new tools for intelligence collection and analysis that must be adopted for us to stay relevant. But they are much more than that. Artificial intelligence, combined with information attacks by authoritarian states, threaten an epistemic storm of disinformation that, ironically, only the use of AI can help solve. Autonomous systems will create new players in the game of intelligence as they become targets and consumers of intelligence. As these technologies revolutionize our economy and society, they will do the same to intelligence.

Our adversaries continue to spy on us as they have for generations, though now adopting their own asymmetric revolutions in intelligence. Russia increasingly turns to covert influence to spread discord among the American people and covert action to attack its enemies. Iran does so as well and uses proxies including Hamas, the Houthis, and Hezbollah to obscure its involvement. North Korea, too, has turned increasingly to cyber warfare. But ultimately, none of these adversaries has the money or power to truly be on the leading edge of intelligence competition.

China is the adversary that poses the primary, existential threat to our way of life, and it is farthest along in its intelligence revolution. It has driven the asymmetric approach to competition and intelligence to its extreme and applied a whole-of-nation approach to intelligence. Its mission is to create a systemic global panopticon of intelligence collection. The Chinese Communist Party has applied this to a system of social credit and information control meant to dominate society. Ultimately, China wants this system to expand globally—to all our phones, college transcripts, health records, and more—as a means to control people and their thoughts. We are all now the targets of intelligence and control. This is a battle between authoritarian governments and civil society. It's a true ideological clash that is as consequential as the Cold War or any conflict that has come before.

This is not just an intelligence competition between great powers; it is a battle between two modes of intelligence. The authoritarian systems rely on dystopian levels of surveillance and human rights abuse. They dismiss the entire concept of personal rights and freedoms in exchange for centrally directed security. At the same time, the authoritarian system attempts to sow social discord, confusion, and disbelief through targeted information attacks. The question for us as we confront this reality and push back against this type of adversary is: What do we want our intelligence system to be like?

When adversaries threaten us and the world changes so, too, must our intelligence, as seen with three intelligence revolutions already in our modern history. The OSS in World War II established the modern intelligence agency in order to fight a global battle. The Cold War professionalized and expanded intelligence in order to compete in the

struggle against the Soviet Union and its deadly KGB. The events of 9/11 expanded intelligence to a whole-of-government approach and drove agencies closer to working with the commercial world in a quest for new technologies and information in order to combat the decentralized international threat of terrorist groups.

At the same time, each of these revolutions has also laid the seeds of the next revolution. The fast and loose approach necessary for the OSS to help win World War II exposed counterintelligence vulnerabilities that the KGB took advantage of in the Cold War. This thereby brought a need for the highly professional, and paranoid, approach by the CIA and other agencies in the Cold War. The compartmentalization of the Cold War led to agencies missing the terrorist threat of 9/11, forcing these agencies to open up and begin to better share intelligence with each other. The centralized, global surveillance put in place after 9/11 has now led to a situation where the sophisticated Chinese intelligence services can parasitically use our surveillance system against us by hacking into our own telecommunication surveillance systems. This asymmetric approach now requires us to develop a new more resilient intelligence system where we can defend ourselves at every level.

Today we stand on the precipice of a fourth revolution in intelligence. In order to combat asymmetric threats from China and other actors, this revolution will expand intelligence farther, to all areas of our society and government; it will involve machines as full partners and, ultimately, will open intelligence to all of us. Just as we once faced the Axis powers and steeled ourselves for the conflict of a world war, today we must do the same.

We cannot ignore the expanded scope of competition and must expand our scope of intelligence along with it, but we must do it the right way. Businesses cannot protect themselves against a nation-state like China. The Intelligence Community has to help. That means intelligence agencies must learn to work with open-source information and recruit and train experts. But it also means that the IC has to learn to partner with the private sector. This is doubly so for S&T intelligence, natural disasters, human rights, and the shared place of outer space. The IC will never replicate the world’s

scientific community, banking industry, or nonprofits inside a classified building; it must learn to work with them.

Doing so requires building trust. Trust requires being more open and exchanging information both ways. This is not about intelligence agencies leaning on laws and threats to force their way in; it is about coming to mutual understanding and exchange to accomplish missions that both sides want, whether that is to stop the next pandemic or to ensure that dictatorial regimes cease genocides. Indeed, it may also require the IC to *not* do certain intelligence missions, but to leave it to civil society to do that work instead, in order to protect rights and build trust. It is only through that trust that we can move from a siloed government agency approach to a whole-of-government, whole-of-nation, and even whole-of-planet strategy.

Artificial intelligence and autonomy may be difficult and even downright scary to implement, but nevertheless, we must embrace their use in a responsible way. The problem of intelligence has shifted from collecting data to analyzing it. If they want to maintain a competitive advantage, intelligence agencies have no choice but to adopt these technologies quickly, serving as collectors, analysts, and customers. It is also necessary to use AI to combat the problems of AI, which include AI-accelerated disinformation and the hacking of the human mind. We, as humans, naturally fear machines having autonomy, as it implies that they have power over us. That is a healthy fear, one that should drive us to ensure that AI and autonomy are adopted in the right way. Responsible adoption of these technologies requires thinking through their effects and developing safety mechanisms. It is not an excuse to use competitive advantage to deny rights; rather, the technologies should be used to further protect those rights and freedoms.

This is not to say that humans will be forced to take a back seat during the fourth intelligence revolution—indeed, we are becoming the primary target, and we must learn to protect ourselves. Our minds are now the battlefield. The fight is over what we know and what we believe. Artificial intelligence tools can help protect us, becoming the bodyguards of our minds. Intelligence agencies can help as well, by realizing that the threat is not just to our presidents and generals, but also to every citizen, and by

working to protect us all. Yet these agencies must be self-limiting in this help: they cannot stray too far toward censorship and otherwise threaten the very rights they were created to protect. We do not want secret police, yet we must protect ourselves from cognitive warfare. This leaves us in a paradoxical position that requires a solution.

As we all become targets of intelligence, we must also become citizen spies. This is the ultimate intelligence revolution—the expansion of intelligence away from intelligence agencies and into the home, from professional intelligence officers to everyone. This could be through forming our own decentralized, citizen intelligence agency, but it could also be through learning about threats from adversaries and then learning how to protect ourselves. As these threats expand into an epistemic storm, learning to tell truth from falsehood will become of utmost importance. These lessons and this training are critical for everyone, especially your children. While it can seem frightening to have to protect oneself, it is also empowering.

Being a citizen spy is an opportunity to directly help our families, our friends, our communities, our nation, and our way of life. It might seem prosaic now to think about changing your password or getting trained to spot phishing scams, but by doing so, you are helping stop cybercriminals. Similarly, helping to halt disinformation will help to stop Chinese, Russian, Iranian, and North Korean spies from trying to tear apart our nation. Knowing how intelligence works and what is at stake and having a say in how our Intelligence Community evolves will make this a better system that is stronger in the end. We can each personally and directly fight back against shadowy attacks on our society.

In the movies, it is field operatives like Jack Bauer and James Bond who are forced to make the hard moral choices in intelligence operations; but today, analysts, software developers, scientists, and everyday citizens must tackle equally thorny ethical decisions. We all make choices every day, small and large, from deciding whether to forward a link, to voting for a leader, to choosing a career. These choices can present real national security—and personal security—dilemmas. Informed voters elect those who make policies governing intelligence operations. We may face

decisions at our office about whether to work on a project for the U.S. government or to accept a demand from a Chinese company. Parents make decisions about what to teach their children. We all must think critically about the information we share. Our intelligence system and, therefore, our national security depend not just on presidents, generals, and intelligence officers, but on us all.

It is also critical that we engage with intelligence to ensure that our intelligence system reflects our values. The United States must fight back against our adversaries, and we must evolve our intelligence system to do so, too. Yet intelligence presents many moral hazards, and it is easy to fall into the trap of evolving to become like your enemy. Everyday citizens must acknowledge what is happening, pay attention, and actively question means and ends. While our government is full of checks and balances, the fundamental check is that of the people. Being the conscience of our intelligence system is ultimately our most important role as citizens.

It may seem like a burden to have to take part in intelligence. No doubt, it would be easier to turn a blind eye to the fact that China is spying on us and trying to establish a global authoritarian government; or, when we hear about another Russian or Iranian election hack, to throw up our hands and say that this future is inevitable and there's nothing we can do. Or perhaps we're sometimes even tempted to drop out of the political process in frustration with our own government and society. But that's a mistake. Taking responsibility and doing your small part is what it means to be a member of a democracy, and it is our moral responsibility. We should not assume that some far-off government agency will take care of it. We are the people, and the government is us.

It is our duty as citizens in a democracy to take on this intelligence role and responsibility. The two modes of intelligence, the autocratic way and the democratic way, stand very differently in moral terms. A liberal democratic intelligence revolution relies on and embraces laws and the protection of rights and freedoms, whereas an autocratic mode dismisses those same laws, freedoms, and responsibilities. But as with everything in a democracy, we are responsible for the outcomes we choose. We vote, we enter politics ourselves, we speak out against injustice, and we volunteer to

protect our country and our communities. Similarly, we all must make an effort to understand what is going on in intelligence, to vote for those we believe will serve us best as leaders, to volunteer, and in some cases to sign on to become professional intelligence officers. However you take part, you maintain the moral responsibility for how intelligence functions. It is in our hands to move toward a distinctly American way of intelligence, one that is open, integrated, technologically grounded, powerful, and, most important, citizen-driven.

From the beginning of this nation, we have all been asked to serve and to help. In 1776, a young teacher from Connecticut, Nathan Hale, joined America's first intelligence and reconnaissance unit, Knowlton's Rangers. General George Washington asked for someone to volunteer to spy behind enemy lines to learn where the British would attempt to invade Manhattan. Hale volunteered, knowing full well that to be caught meant death. After being captured, Hale, while standing on the gallows on September 22, 1776, was reported to have uttered, "I only regret, that I have but one life to lose for my country." Today we confront new threats to our nation. We are not being asked to have two lives to lose for our country, but rather two lives to give. One life is devoted to our home and work. The other is dedicated to safeguarding ourselves, our families, our communities, and our nation. This is the essence of being a citizen spy.

We are all intelligence officers now, and we must know the truth. For the truth will keep us free.

OceanofPDF.com

Notes

The page numbers for the notes that appeared in the print version of this title are not in your e-book. Please use the search function on your e-reading device to search for the relevant passages documented or discussed.

Prologue

“The future is already here”: William Gibson, “The Science in Science Fiction,” NPR, October 22, 2018, https://www.npr.org/2018/10/22/1067220/the-science-in-science-fiction.

Introduction

“If we were to attempt”: Robert Cardillo, “Remarks as Prepared for Delivery by Robert Cardillo Director, National Geospatial-Intelligence Agency Small Satellites—Big Data,” August 7, 2017, https://www.nga.mil/news/Small_Satellites_-_Big_Data.html.

China: A note on my use of “China.” Throughout this book, I will refer to “China,” “the Chinese,” and “the Chinese Communist Party” (CCP) more or less interchangeably. In almost all cases, I am referring to the Chinese system of government and its decision makers. The Chinese people, the public, are not making decisions, as might be said in a democratic government, and don’t have direct responsibility for most of the decisions that are made. If I am referring specifically to the Chinese people as a population or group, I will point that out. The same goes for Russia and other nations.

Intelligence concerns information: This is my own simplified view of what intelligence is about. There is a whole cottage industry for defining what intelligence is. If you want something more official, the director of national intelligence, the highest-ranking official in the Intelligence Community, defines intelligence as “information gathered within or outside the United States that involves threats to our nation, its people, property, or interests; development, proliferation, or use of weapons of mass destruction; and any other matter bearing on the U.S. national or homeland security. Intelligence can provide insights not available elsewhere that warn of potential threats and opportunities, assess probable outcomes of proposed policy options, provide leadership profiles on foreign officials, and inform official travelers of counterintelligence and security threats.” Office of the Director of National Intelligence, “What Is Intelligence?” https://www.dni.gov/index.php/what-we-do/what-is-intelligence.

“whoever fights monsters”: Friedrich Nietzsche, *Beyond Good and Evil* (Penguin Press, 2003).

Chapter 1: The Heroic Age

"The necessity of procuring": *The Evolution of the U.S. Intelligence Community—An Historical Overview* (U.S. Government Printing Office, n.d.), https://www.govinfo.gov/content/pkg/GPO-INTELLIGENCE/html/int022.html.

"secret correspondence": *The Evolution of the U.S. Intelligence Community*.

Congress agreed: *The Evolution of the U.S. Intelligence Community*.

"Gentlemen do not read": Henry L. Stimson and McGeorge Bundy, *On Active Service in Peace and War* (Harper, 1947), 194, 188, https://archive.org/details/onactiveservices006603mbp/page/188/mode/2up?view=theater.

no permanent intelligence office until 1882: *The Evolution of the U.S. Intelligence Community.*

Between the world wars: John Whiteclay Chambers II, "Wild Bill Donovan and the Origins of the OSS," National Park Service, U.S. Department of the Interior, https://home.nps.gov/prwi/learn/historyculture/donovan.htm.

On one such mission: Chambers II, "Wild Bill Donovan and the Origins of the OSS."

Even as Donovan: Chambers II, "Wild Bill Donovan and the Origins of the OSS."

in the Social Register: Michael Pearson, "Wild Bill Donovan," *Vanity Fair*, March 2011, https://www.vanityfair.com/culture/2011/03/wild-bill-donovan201103.

"the glorious amateurs": Susan L. Kerr and John D. Gresham, *The OSS Society: Keepers of Gen. Donovan's Flame* (OSS Society, 2010), https://osssociety.org/pdfs/YISO2010.pdf.

Julia Child: Lisa Hagan, *Sisterhood of Spies: The Women of the OSS*, repr. ed. (Naval Institute Press, 2009).

Secret Intelligence: U.S. Army Special Operations Command (USASOC), "OSS Legacy," https://www.soc.mil/OSS/oss-legacy.html.

From this politically neutral: Stephen Kinzer, *The Brothers: John Foster Dulles, Allen Dulles, and Their Secret World War*, revised and enlarged ed. (Henry Holt and Company, 2013).

Obergruppenführer Karl Wolff: National World War II Museum, "The Spy Who Captured an Army," https://www.nationalww2museum.org/war/articles/wwii-spy-allen-dulles.

Aaron Bank: Aaron Bank, *From OSS to Green Beret* (Pocket, 1987).

Harvard historian William Langer: Harvard Square Library, "Langer, William L. (1896–1977)," https://www.harvardsquarelibrary.org/biographies/william-l-langer/.

including Harvard and Columbia: See, for example, Bruce Cumings, "Biting the Hand that Feeds You: Why the 'Intelligence Function' of American Foundation Support for Area Studies Remains Hidden in Plain Sight," Global Society, January 27, 2024.

suitcase-portable radios: National Park Service, "A Wartime Organization for Unconventional Warfare," https://www.nps.gov/articles/a-wartime-organization-for-unconventional-warfare.htm.

Lambertsen Amphibious Respiratory Unit: Patrick K. O'Donnell, *First SEALs: The Untold Story of the Forging of America's Most Elite Unit* (Henry Holt and Company, 2014).

Navy SEALs: Articles of War Studies Online, "OSS Maritime Operations," https://arsof-history.org/articles/v1n2_oss_maritime_page_1.html.

Newly inaugurated president Harry Truman: Scott A. Moseman, “Truman and the Formation of the Central Intelligence Agency,” *Journal of Intelligence History* 19, no. 2 (2020): 151.

“Gestapo”: Moseman, “Truman and the Formation of the Central Intelligence Agency,” 151–53.

Chapter 2: The Golden Age

After thirteen consecutive: See, for example, Center for the Study of National Reconnaissance, National Reconnaissance Office, "The CORONA Story," https://www.nro.gov/Portals/135/documents/history/csnr/corona/The%20CORONA%20Story.pdf?ver=BgSn5nPYz45EZ9O_ZF57Ow%3d%3d.

By the summer of 1962: Joseph W. Caddell, "Corona over Cuba: The Missile Crisis and the Early Limitations of Satellite Imagery Intelligence," *Intelligence and National Security* 31, no. 3 (2016): 417.

The Farm, where I was trained: See, for example, Miles Copeland, "Down on 'the Farm' in Virginia," *Richmond Times Dispatch*, August 25, 1974, https://www.cia.gov/readingroom/docs/CIA-RDP88–01350R000200810007–8.pdf; Amaryllis Fox, "This Is How You Train as a Spy in the CIA's Most Elite Covert Unit," *Washingtonian*, October 13, 2019, https://www.washingtonian.com/2019/10/13/amaryllis-fox-how-you-train-spy-cia-most-elite-covert-unit/; Greg Miller, "DIA to Send Hundreds More Spies Overseas," *Washington Post*, December 1, 2012, https://www.washingtonpost.com/world/national-security/dia-to-send-hundreds-more-spies-overseas/2012/12/01/97463e4e-399b-11e2-b01f-5f55b193f58f_story.html.

CIA agents and, later: Miller, "DIA to Send Hundreds More Spies Overseas."

Project Azorian: Central Intelligence Agency, *Office of Strategic Services*, https://www.cia.gov/resources/csi/static/Office-of-Strategic-Services.pdf; "Voyage to the Bottom of the Sea—The CIA Mission to Raise a Soviet Sub," Articles of Defense Studies Today, August 2016, https://adst.org/2016/08/voyage-bottom-sea-cia-mission-raise-soviet-sub/.

"an intelligence discipline": Office of the Director of National Intelligence, *MASINT Primer_V5_2022*, https://www.dni.gov/files/ODNI/documents/21–113_MASINT_Primer__2022.pdf.

"damage": U.S. Army Information Security, "Classification Levels," https://www.dami.army.pentagon.mil/site/infosec/TP-levels.aspx.

Chapter 3: The Chaotic Age

“extraordinary rendition”: Dan Bilefsky, “Court Censures Poland over CIA Renditions,” *New York Times*, July 24, 2014, https://www.nytimes.com/2014/07/25/world/europe/europe-poland-cia-black-site-extraordinary-rendition.html.

MQ-1 Predator: Robert Windrem, “How the Predator Went from Eye in the Sky to War on Terror’s Weapon of Choice,” NBC News, https://www.nbcnews.com/news/investigations/how-predator-went-eye-sky-war-terrors-weapon-choice-flna6c10215303.

“targeted killing”: Mark Mazzetti, “A Secret Deal on Drones, Sealed in Blood,” *New York Times*, April 6, 2013, https://www.nytimes.com/2013/04/07/world/asia/origins-of-cias-not-so-secret-drone-war-in-pakistan.html.

As the National: National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, 2004.

Back in October 2000: OARDEC, “Summary of Evidence for Combatant Status Review Tribunal—Bin Attash, Walid Muhammad Salih,” Department of Defense Office for the Administrative Review of the Detention of Enemy Combatants at U.S. Naval Base Guantanamo Bay, Cuba, February 8, 2007.

The CIA, investigating: J. Gilmore, “What If…?” *Frontline*, PBS, October 4, 2002, https://www.pbs.org/wgbh/frontline/article/what-if/.

In another episode: Office of the Inspector General, “Chapter Five: Two September 11 Hijackers: Khalid Al-Mihdhar and Nawaf Al-Hazmi,” *A Review of the FBI’s Handling of Intelligence Information Prior to the September 11 Attacks: Special Report*, November 2004 (released publicly June 2005), https://oig.justice.gov/sites/default/files/archive/special/0506/chapter5.htm.

In 2010, Saudi Arabia: Eric Schmitt and Scott Shane, “Saudis Warned US of Attack Before Parcel Bomb Plot,” *New York Times*, November 5, 2010.

In 2017, the CIA: “Trump Putin Call: CIA Helped Stop Russia Terror Attack,” BBC, December 7, 2017.

Chapter 4: Asymmetric Adversaries

“Immediately felt like”: Anton Troianovski, “A Former Russian Troll Speaks: ‘It Was Like Being in Orwell’s World,’” *Washington Post*, February 17, 2018, https://www.washingtonpost.com/news/worldviews/wp/2018/02/17/a-former-russian-troll-speaks-it-was-like-being-in-orwells-world/.

“Defendant ORGANIZATION”: U.S. Department of Justice, “Internet Research Agency Indictment,” February 16, 2018, https://www.justice.gov/d9/fieldable-panel-panes/basicpanes/attachments/2018/02/16/internet_research_agency_indictment.pdf.

Using an estimated one hundred thousand dollars: Scott Shane and Vindu Goel, “Fake Russian Facebook Accounts Bought $100,000 in Political Ads,” *New York Times*, September 6, 2017.

To fund its nuclear program: Michelle Nichols, “UN Experts Investigate 58 Cyber Attacks Worth $3 Billion by North Korea,” Reuters, February 8, 2024, https://www.reuters.com/technology/cybersecurity/un-experts-investigate-58-cyberattacks-worth-3-bln-by-north-korea-2024–02–08/.

Chapter 5: Enemy Number One

After traveling around: "China Surprises U.S. with Hypersonic Missile Test, FT Reports," Reuters, October 17, 2021, https://www.reuters.com/world/china-surprises-us-with-hypersonic-missile-test-ft-reports-2021–10–17/; Emma Helfrich and Tyler Rogoway, "More Details on China's Exotic Orbital Hypersonic Weapon Come to Light," The War Zone, https://www.twz.com/more-details-on-chinas-exotic-orbital-hypersonic-weapon-come-to-light.

"I don't know if it's quite": Jennifer Grewing, "'It Did Circle the Globe': US Confirms China's Orbital Hypersonic Test," Defense One, October 21, 2021, https://www.defenseone.com/threats/2021/10/it-did-circle-globe-us-confirms-chinas-orbital-hypersonic-test/186407/.

It's been estimated that sixteen: Minxin Pei, *The Sentinel State: Surveillance and the Survival of the Dictatorship in China* (Harvard, 2024).

an estimated thirteen million people: Pei, *The Sentinel State*.

Personal Information Protection Law: "Personal Information Protection Law of the People's Republic of China," National People's Congress of the People's Republic of China, December 2021, http://en.npc.gov.cn.cdurl.cn/2021–12/29/c_694559.htm.

"any organization or citizen": Arjun Kharpal, "Huawei Says It Would Never Hand Data to China's Government. Experts Say It Wouldn't Have a Choice," CNBC, March 5, 2019, https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html.

since 2018: See, for example, "Chinese Communist Party Cells in Private Companies: Though Not Yet Universal, Increasingly Situated to Play Greater Roles in Corporate Governance," Sayari, April 7, 2021, https://sayari.com/resources/chinese-communist-party-cells-in-private-companies-though-not-yet-universal-increasingly-situated-to-play-greater-roles-in-corporate-governance/.

Securities Regulatory Commission: Jill Goldenziel, "Chinese Communist Party Demands Employees at Western Firm Show Their Support," *Forbes*, February 27, 2023, https://www.forbes.com/sites/jillgoldenziel/2023/02/27/chinese-communist-party-demands-employees-at-western-firm-show-their-support/.

CCP members: Goldenziel, "Chinese Communist Party Demands Employees at Western Firm Show Their Support."

He later reappeared in Japan: Casey Hall, "Alibaba's Jack Ma Steps Out from the Shadows with Morale-Boosting Post," Reuters, April 10, 2024, https://www.reuters.com/business/retail-consumer/alibaba-founder-jack-ma-steps-out-shadows-with-long-internal-post-2024–04–10/.

"social credit score": Nicole Kobie, "The Complicated Truth About China's Social Credit System," *Wired UK*, January 24, 2019, https://www.wired.com/story/china-social-credit-score-system/; Brittany Mears, "China's Social Credit System: Speculation vs. Reality," *Diplomat*, March 3, 2021; https://thediplomat.com/2021/03/chinas-social-credit-system-speculation-vs-reality/; Simina Mistreanu, "Life Inside China's Social Credit Laboratory," *Foreign Policy*, April 3, 2018, https://www.emerald.com/insight/content/doi/10.1108/MIP-06–2017–0100/full/html.

a story or even a word: Xiaofeng Wang et al., "The Velocity of Censorship: High-Fidelity Detection of Microblog Post Deletions," arXiv preprint arXiv:1303.0597, March 2013, https://arxiv.org/ftp/arxiv/papers/1303/1303.0597.pdf.

While Chinese internal data: David E. Sanger and Shane Harris, “China Harvests Masses of Data on Western Targets, Documents Show,” *Washington Post*, December 31, 2021, https://www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html.

Though it denies it: David McCabe and Sapna Maheshwari, “US Sues TikTok over Child Privacy Violations,” *New York Times*, August 2, 2024.

despite repeated denials: Kharpal, “Huawei Says It Would Never Hand Data to China’s Government.”

In 2015, China: Ellen Nakashima, “Chinese Breach Data of 4 Million Federal Workers,” *Washington Post*, June 4, 2015, https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52–0af7–11e5–95fd-d580f1c5d44e_story.html.

“Through its cyber intrusions”: Office of the Director of National Intelligence, “China’s Collection of Genomic and Healthcare Data: Risks to Privacy and U.S. National Security,” National Counterintelligence and Security Center, February 2021, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact_Sheet_2021revision20210203.pdf.

Salt Typhoon: Sarah Krouse et al., “US Wiretap Systems Targeted in China-Linked Hack,” *Wall Street Journal*, October 5, 2024, https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b?mod=article_inline.

targeted the phones of Donald Trump: Ellen Nakashima and Josh Dawsey, “Chinese Hackers Said to Have Collected Audio of American Calls,” *Washington Post*, October 27, 2024, https://www.washingtonpost.com/national-security/2024/10/27/chinese-hackers-cellphones-trump/.

“China’s BGI”: Office of the Director of National Intelligence, “China’s Collection of Genomic and Healthcare Data: Risks to Privacy and U.S. National Security.”

“Chinese companies have”: Office of the Director of National Intelligence, “China’s Collection of Genomic and Healthcare Data: Risks to Privacy and U.S. National Security.”

Cognizant of the threat: The White House, “Executive Order on Preventing Access to Americans’ Bulk Sensitive Personal Data and United States Government–Related Data by Countries of Concern,” February 28, 2024, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/.

For some time, this has: Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: Two Air Force Senior Colonels on Scenarios for War and the Operational Art in an Era of Globalization* (People’s Liberation Army Literature and Arts Publishing House, 1999).

In 2024, around seven hundred: John Ruwitch, “Why the Number of American Students Choosing to Study in China Remains Low,” *Morning Edition*, NPR, June 13, 2024, https://www.npr.org/2024/06/13/nx-s1–4989350/why-the-number-of-american-students-choosing-to-study-in-china-remains-low.

“handsome men and beautiful women”: Bernard Orr and Kim Coghill, “China Warns Students ‘Beautiful Women, Handsome Guys’ Could Lure Them into Spying,” Reuters, September 4, 2024,

https://www.reuters.com/world/china/china-warns-students-beautiful-women-handsome-guys-could-lure-them-into-spying-2024–09–04/.

“build a people’s”: Chun Han Wong, “A Xi Enforcer Is Revving Up China’s Spy Machine—and Alarming the West,” *Wall Street Journal*, November 9, 2024, https://www.wsj.com/world/china/a-xi-enforcer-is-revving-up-chinas-spy-machineand-alarming-the-west-6b87999f?mod=mhp.

Its secret services are said: Max Colchester and Daniel Michaels, “Scale of Chinese Spying Overwhelms Western Governments,” *Wall Street Journal*, October 14, 2024, https://www.wsj.com/politics/national-security/scale-of-chinese-spying-overwhelms-western-governments-6ae644d2?mod=mhp.

Chapter 6: Embracing Economic Espionage

Zhang Hao: U.S. Department of Justice, "Chinese Citizen Sentenced for Economic Espionage, Theft of Trade Secrets, and Conspiracy," U.S. Department of Justice, September 1, 2020, https://www.justice.gov/usao-ndca/pr/chinese-citizen-sentenced-economic-espionage-theft-trade-secrets-and-conspiracy.

"If a beach was": Peter Mattis, "A Guide to Chinese Intelligence Operations," War on the Rocks, August 18, 2015, https://warontherocks.com/2015/08/a-guide-to-chinese-intelligence-operations.

Hambantota Port in Sri Lanka: Maria Abi-Habib, "How China Got Sri Lanka to Cough Up a Port," *New York Times*, June 25, 2018, https://www.nytimes.com/2018/06/25/world/asia/china-sri-lanka-port.html.

China mines 60 percent: Graceline Baskaran, "What China's Ban on Rare Earths Processing Technology Exports Means," CSIS, January 8, 2024, https://www.csis.org/analysis/what-chinas-ban-rare-earths-processing-technology-exports-means#:~:text=At%20present%20China%20produces%2060,given%20China%20a%20near%20monopoly.

Israel was able: Maya Gebeily, James Pearson, and David Gauthier-Villars, "How Israel's Bulky Pager Fooled Hezbollah," Reuters, October 15, 2024, https://www.reuters.com/graphics/ISRAEL-PALESTINIANS/HEZBOLLAH-PAGERS/mopawkkwjpa/.

17,500 intelligence officers: U.S. Army Intelligence and Security Command, March 15, 2025, https://www.usainscom.army.mil/MSCs/.

Committee of Secret Correspondence: William Carmichael, "To the Committee of Secret Correspondence v3:477," November 2, 1776, reprinted by Northern Illinois University Digital Library, https://digital.lib.niu.edu/islandora/object/niu-amarch%3A79612.

"We know more about Soviet grain": Stansfield Turner, "Remarks," West Point Senior Conference, United States Military Academy, West Point, NY, June 9, 1990.

When Guatemala's democratically: Laura Moye, "The United States Intervention in Guatemala," *International Social Science Review* 73, no. 1/2 (1998): 45–47.

Office of Commercial and Economic Analysis: https://www.afocea.com.

National Economic Defense Center: Anthony Vinci, "Competitive Climate: America Must Counter China's Investing in Economic Intelligence," The National Interest, https://nationalinterest.org/feature/competitive-climate-america-must-counter-china-investing-economic-intelligence-120356.

Open Source Enterprise: Emily Harding, "The IC's New Open Source Strategy Gets the Basics Right," Center for Strategic and International Studies, April 2, 2024, https://www.csis.org/analysis/ics-new-osint-strategy-gets-basics-right.

At the NGA, we had a program called Pathfinder: Regina Galvin, "NGA Open for Business," NGA Office of Corporate Communication, May 27, 2015, https://www.nga.mil/news/NGA_Open_for_Business.html.

As with JASON: I have proposed and worked on such a concept with MITRE Corp.

CEO of Rheinmetall: Katie Bo Lillis, Natasha Bertrand, and Frederik Pleitgen, "Exclusive: US and Germany Foiled Russian Plot to Assassinate CEO of Arms Manufacture Sending Weapons to

Ukraine," CNN, July 11, 2024, https://www.cnn.com/2024/07/11/politics/us-germany-foiled-russian-assassination-plot/index.html?utm_source=sailthru&utm_medium=email&utm_campaign=mil-ebb.

intelligence ecosystem: William Schlickenmaier and Anthony Vinci, working paper on the intelligence ecosystem, 2024.

Chapter 7: From National Security to Global Security

"computerize disease information": ABC News, "Project Impact: Disease Intelligence and How the CIA Traced Epidemics out of Cold War Asia," ABC News, June 20, 2020, https://abcnews.go.com/Politics/project-impact-disease-intelligence-cia-traced-epidemics-cold/story?id=71299224.

BLACKFLAG successfully monitored: ABC News, "Project Impact."

"a cataclysmic event": Darren Baker and Luke Mickelson, "Intelligence Report Warned of Coronavirus Outbreak, Sources Say," ABC News, May 14, 2020, https://abcnews.go.com/Politics/intelligence-report-warned-coronavirus-crisis-early-november-sources/story?id=70031273.

director of the Wuhan Central Hospital: Annie Sparrow, "China Hid Early Warnings About Covid-19, Costing Lives of Health Care Workers Worldwide," *Foreign Policy*, March 18, 2021, https://foreignpolicy.com/2021/03/18/china-covid-19-killed-health-care-workers-worldwide/.

"It may have been a reluctance": Sparrow, "China Hid Early Warnings About Covid-19, Costing Lives of Health Care Workers Worldwide."

two trillion dollars: Eduardo Levy Yeyati and Federico Filippini, "Social and Economic Impact of COVID-19," Brookings Institute, June 8, 2021, https://www.brookings.edu/articles/social-and-economic-impact-of-covid-19/.

this system was not dismantled: Chauncey Jung, "China's Political Surveillance System Keeps Growing," *Diplomat*, June 23, 2022, https://thediplomat.com/2022/06/chinas-political-surveillance-system-keeps-growing/.

anniversary of the Tiananmen: Marc Lynch, "China Is Using COVID-19 to Throttle Hong Kong's Pro-Democracy Movement," *Washington Post*, May 21, 2020, https://www.washingtonpost.com/washington-post-live/2023/11/30/hong-kong-china-threats-global-democracy/.

Between 2003 and 2008: United States Holocaust Memorial Museum, "Darfur," *United States Holocaust Memorial Museum Encyclopedia*, https://www.ushmm.org/genocide-prevention/countries/sudan.

"began as an ecological crisis": Ban Ki-moon, "A Climate Culprit in Darfur," United Nations, June 16, 2007, https://www.un.org/sg/en/content/sg/articles/2007–06–16/climate-culprit-darfur.

Others have noted: Vikram Mansharamani, "A Major Contributor to the Syrian Conflict? Climate Change," *PBS NewsHour*, PBS, March 16, 2016, https://www.pbs.org/newshour/economy/a-major-contributor-to-the-syrian-conflict-climate-change.

the CIA set up a Center: Central Intelligence Agency, "Press Release: CIA Opens Center on Climate Change and National Security," September 25, 2009, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB54/docs/doc_61.PDF.

The U.S. National Science Foundation: American Institute of Physics, "FY23 Budget Outcomes: National Science Foundation," *American Institute of Physics*, February 10, 2023, https://ww2.aip.org/fyi/fy2023-national-science-foundation.

Meanwhile, an intelligence office like: Jonathan Clemente, "Medical Intelligence," *Intelligencer: Journal of U.S. Intelligence Studies* 20, no. 2 (Fall/Winter 2023): 73–78,

https://www.afio.com/publications/CLEMENTE%20Pages%20from%20INTEL_FALLWINTER2013_Vol20_No2.pdf.

the CIA set up the: William Broad, "CIA Is Sharing Data with Climate Scientists," *New York Times*, January 4, 2010, https://www.nytimes.com/2010/01/05/science/earth/05satellite.html.

show mass graves in Iran: Erin Cunningham and Dalton Bennett, "Coronavirus Burial Pits So Vast They're Visible from Space," *Washington Post*, March 12, 2020, https://www.washingtonpost.com/graphics/2020/world/iran-coronavirus-outbreak-graves/.

The U.S. government has declassified: Mariah Petrovic, "Reveal: Cold War Spy Imagery Now Helping Fight Climate Change," ESRI, May 6, 2021, https://www.esri.com/about/newsroom/blog/cold-war-spy-imagery/?srsltid=AfmBOopdW5W0982Np5OfYLUFPxGKuCrItxSvFDjvaEKwJXqXsIDifHoj.

There were beneficial impacts: Xu Xiao et al., "US Embassy Air-Quality Tweets Led to Global Health Benefits," *Proceedings of the National Academy of Sciences* 120, no. 11 (March 2023): e2201092119, https://www.pnas.org/doi/full/10.1073/pnas.2201092119.

during the Cold War détente: Central Intelligence Agency, *Soviet Dissent and Its Repression Since the 1975 Helsinki Accords*, National Security Archive, July 10, 1985, https://nsarchive.gwu.edu/sites/default/files/documents/2839067/Document-6.pdf.

Tearline, a program: National Geospatial-Intelligence Agency, "About Tearline," https://www.tearline.mil/about-tearline.

Through this initiative: National Geospatial-Intelligence Agency, "About Tearline."

The RAND Corporation: Katherine Pfrommer and Ed Burke, "Geolocating Explosive Growth in Preschools in Western China Due to 'Re-education' Policies," National Geospatial-Intelligence Agency, April 16, 2020.

Another group, at the University of Texas: National Geospatial-Intelligence Agency, *"Trust But Verify": Analyzing Refugee Vehicle Movements in Eastern Ukraine*, May 2022, https://www.tearline.mil/public_page/refugee-vehicle-movements-in-eastern-ukraine.

Chapter 8: The Final Frontier of Intelligence

the *New York Times* reported: Tim Weiner, “Ultra-Secret Office Gets First Budget Scrutiny,” *New York Times*, August 10, 1994, https://www.nytimes.com/1994/08/10/us/ultra-secret-office-gets-first-budget-scrutiny.html.

On top of that, Space Force: Department of Defense, “FY-25 Posture Statement,” U.S. Air Force, September 19, 2023, https://www.af.mil/Portals/1/documents/2024SAF/FY25_Posture_Statement.pdf.

By 2024: Union of Concerned Scientists, UCS Satellite Database, https://www.ucsusa.org/resources/satellite-database.

we signed a $14 million: Kendall Russell, “NGA Purchases $14 Million, One-Year Subscription to Planet Imagery,” Via Satellite, July 21, 2017, https://www.satellitetoday.com/government-military/2017/07/21/nga-purchases-14-million-one-year-subscription-planet-imagery/.

Starshield business unit: Joey Roulette and Marisa Taylor, “Exclusive: Musk’s SpaceX Is Building Spy Satellite Network for US Intelligence Agency, Sources Say,” Reuters, March 16, 2024, https://www.reuters.com/technology/space/musks-spacex-is-building-spy-satellite-network-us-intelligence-agency-sources-2024–03–16/.

“the most capable, diverse”: Roulette and Taylor, “Musk’s SpaceX Is Building Spy Satellite Network for US Intelligence Agency.”

“Space is the world’s newest”: “Trump Signs Law Establishing U.S. Space Force,” U.S. Department of Defense, December 20, 2019, https://www.defense.gov/News/News-Stories/article/article/2046035/trump-signs-law-establishing-us-space-force/.

“Know the World”: National Geospatial-Intelligence Agency, “Mission,” https://www.nga.mil/about/Mission.html.

Chapter 9: Genetic Espionage

“can detect Down”: “The New NIFTY-pro Test,” https://niftytest-ce.eu/#:~:text=NIFTY™%20(Non%2DInvasive%20Fetal,abnormalities%20and%20microdeletion%2Fmicroduplication%20syndromes.

The development of the test: Kristy Needham and Clare Baldwin, “China’s Gene Giant Harvests Data from Millions of Women,” Reuters, July 7, 2021, https://www.reuters.com/investigates/special-report/health-china-bgi-dna/.

“improving population quality”: Needham and Baldwin, “China’s Gene Giant Harvests Data from Millions of Women.”

In 2023, there were reports: Daniel Boffey, “Chinese Firm Got COVID Contract Despite Trying to Hack NHS Data, Minister Says,” *Guardian*, March 8, 2023, https://www.theguardian.com/politics/2023/mar/08/mps-call-for-uk-to-ban-chinese-gene-research-firm-from-government-contracts-bgi-group.

The Pentagon and IC: Joby Warrick and Cate Brown, “China’s Quest for Human Genetic Data Spurs Fears of a DNA Arms Race,” *Washington Post*, September 21, 2023, https://www.washingtonpost.com/world/interactive/2023/china-dna-sequencing-bgi-covid/.

It reportedly sold test: Warrick and Brown, “China’s Quest for Human Genetic Data Spurs Fears of a DNA Arms Race.”

Complete Genomics: Warrick and Brown, “China’s Quest for Human Genetic Data Spurs Fears of a DNA Arms Race.”

Human Rights Watch: “China: Minority Region Collects DNA from Millions,” Human Rights Watch, December 13, 2017, https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions.

a major U.S. genetics: Rebecca Carballo, Emily Schmall, and Remy Tumin, “23andMe Breach Targeted Jewish and Chinese Customers, Lawsuit Says,” *New York Times*, January 26, 2024, https://www.nytimes.com/2024/01/26/business/23andme-hack-data.html.

In fact, in 2023: “Healthcare Data Breach Statistics,” *HIPAA Journal*, https://www.hipaajournal.com/healthcare-data-breach-statistics/.

One example is a microbe: “Strain Improvement for Sustainable Agriculture with Bayer,” Ginkgo Bioworks, https://www.ginkgobioworks.com/case-studies/bayer/.

In 2018, Chinese researcher: Heidi Ledford, “First Gene-Edited Babies Allegedly Born,” *Chemical & Engineering News* 96, no. 48 (2018), https://cen.acs.org/policy/First-gene-edited-babies-allegedly/96/i48.

“conducting illegal medical”: Dennis Normile, “Chinese Scientist Who Produced Genetically Altered Babies Sentenced to 3 Years in Jail,” *Science*, December 30, 2019, https://www.science.org/news/2019/12/chinese-scientist-who-produced-genetically-altered-babies-sentenced-3-years-jail.

In 1998: Chandré Gould and Peter Folb, *Project Coast: Apartheid’s Chemical and Biological Warfare Programme*, ed. Robert Berold (United Nations, 2002).

“These weapons included”: Gould and Folb, *Project Coast.*

In some research, China: Needham and Baldwin, “China’s Gene Giant Harvests Data from Millions of Women.”

enhance soldiers’ performance: Needham and Baldwin, “China’s Gene Giant Harvests Data from Millions of Women.”

One concept: Matt McKnight and Anthony Vinci, working paper on biosecurity, 2024.

To take advantage of the Germans’: Nazi War Crimes Interagency Working Group, Declassified Records, National Archives, https://www.archives.gov/iwg/declassified-records/rg-330-defense-secretary.

Operation Paperclip brought German: Annie Jacobsen, *Operation Paperclip: The Secret Intelligence Program that Brought Nazi Scientists to America* (Little, Brown and Company, 2014).

It’s been reported: William Hannas and Chang Huey-Meei, “China’s STI Operations: Monitoring Foreign Science and Technology Through Open Sources,” Center for Security and Emerging Technology (CSET), January 2021, https://cset.georgetown.edu/publication/chinas-sti-operations/.

The CIA had been tracking: Amy Ryan and Gary Keeley, “Sputnik and US Intelligence: The Warning Record,” *Studies in Intelligence* 61, no. 3 (September 2017), https://www.cia.gov/resources/csi/static/Sputnik-and-US-Intel.pdf.

Developed under the Reagan administration: See, for example, Mike Sekora, “Towards a Technology-Based Strategy,” Trade Reform, August 27, 2010, https://web.archive.org/web/20110126130501/http://www.tradereform.org/2010/08/mike-sekora-towards-a-technology-based-strategy/; John Markoff, “The High-Tech Future,” *New York Times*, May 24, 1990, https://www.nytimes.com/1990/05/24/opinion/in-the-nation-the-high-tech-future.html?pagewanted=all; Michael Sekora, “An Unfinished Legacy: President Reagan and the Socrates Project,” *Daily Caller*, December 6, 2010, https://dailycaller.com/2010/12/06/an-unfinished-legacy-president-reagan-and-the-socrates-project/.

While the prospect of predicting: See, for example, Kevin Kelly, *What Technology Wants: An Illustrated Paperback* (Penguin Books, 2011); and Matt Ridley, *How Innovation Works: And Why It Flourishes in Freedom* (Harper, 2020).

The CIA funded: Nicholas B. Dirks, “Scholars, Spies, and Global Studies,” *The Chronicle of Higher Education*, August 13, 2012, https://www.chronicle.com/article/scholars-spies-and-global-studies/.

Intelligence agencies have also carried out covert: Mike Shuster, “Inside the United States Secret Sabotage of Iran,” NPR, May 9, 2011, https://www.npr.org/2011/05/09/135854490/inside-the-united-states-secret-sabotage-of-iran; Ronan Bergman and Farnaz Fassihi, “The Scientist and the A. I. Assisted, Remote Controlled Killing Machine,” *New York Times*, September 18, 2021, https://www.nytimes.com/2021/09/18/world/middleeast/iran-nuclear-fakhrizadeh-assassination-israel.html.

Chapter 10: The Rise of AI

They were initially built: Jeffrey Lewis, “That Ain’t My Truck: Where North Korea Assembled Its Chinese Transporter-Erector-Launchers,” 38 North, February 3, 2014, https://www.38north.org/2014/02/jlewis020314/.

NASA tells us: NASA Earth Observatory, Cloudy Earth, n.d.

parallel intelligence: Jason Bruzdzinski, “Striving for Cognitive Superiority in the 3rd IT Age: The New Wars and Means of Intelligence Analysis,” National Academies of Sciences, Engineering and Medicine, YouTube video, July 29, 2024, https://www.youtube.com/watch?v=SCtZoCxPqzQ.

“Whoever becomes the leader”: “AI to Rule the World? Putin Says No to Risky Tech Race,” RT.com, February 20, 2020, https://www.rt.com/news/401731-ai-rule-world-putin/.

Chapter 11: From Augmenting to Automating Intelligence

In 2017, we started Data Corps: NGA Office of Corporate Communications, "Q&A with NGA's Chief Data Scientist," *Medium*, February 15, 2018, https://medium.com/@NGA_GEOINT/q-a-with-ngas-chief-data-scientist-d6decc94451b.

Alphabet's Jigsaw: Gillian Tett, "The Human Factor—Why Data Is Not Enough to Understand the World," *Financial Times*, May 28, 2021, https://www.ft.com/content/4f00469c-75da-4e29-baf3-b7bec470732c; Jigsaw, "7 Insights from Interviewing Conspiracy Theory Believers," Medium, July 12, 2018, https://medium.com/jigsaw/7-insights-from-interviewing-conspiracy-theory-believers-c475005f8598.

For example, the company Anthropic: Anthropic, "Mapping the Mind of a Large Language Model," Medium, May 21, 2024, https://www.anthropic.com/research/mapping-mind-language-model.

In 2024, MITRE launched: MITRE Corp., "MITRE Opens New AI Assurance and Discovery Lab," May 25, 2024, https://www.mitre.org/news-insights/news-release/mitre-opens-new-ai-assurance-and-discovery-lab.

machine learning poisoning: Alexey Kurakin, Ian Goodfellow, and Samy Bengio, "Explaining and Harnessing Adversarial Examples," arXiv preprint arXiv: 1412.6572, March 20, 2015, https://arxiv.org/abs/1412.6572.

The proof of concept for this danger came in 2018: Scott Shane and Daisuke Wakabayashi, "'The Business of War': Google Employees Protest Work for the Pentagon," *New York Times*, April 4, 2018, https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html.

Chapter 12: Singularity War

But this dogfight: Lt. Col. Ryan Hefron, "Air Combat Evolution (ACE)," DARPA, n.d.; Tim McMillan, "DARPA's Groundbreaking 'ACE' Program and X-62A Becomes First AI-Controlled Jet to Dogfight Against Manned F16 in Real World," The Debrief, April 17, 2024, https://thedebrief.org/darpas-groundbreaking-ace-program-and-x-62a-becomes-first-ai-controlled-jet-to-dogfight-against-manned-f-16-in-real-world/.

Edward Luttwak: Edward N. Luttwak, *Strategy: The Logic of War and Peace*, rev. and enlarged ed. (Harvard University Press, 2009).

All I have to do: William Goldman, *The Princess Bride* (Act III Communications, Buttercup Films. 1987).

Algorithmic Warfare Cross-Functional Team: See, for example, Robert Work, "Memorandum: Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)," Department of Defense. April 26, 2017, https://www.govexec.com/media/gbc/docs/pdfs_edit/establishment_of_the_awcft_project_maven.pdf ; Gregory Allen, "Project Maven Brings AI to the Fight Against ISIS," CNAS, December 21, 2017, https://www.cnas.org/publications/commentary/project-maven-brings-ai-to-the-fight-against-isis; and Cheryl Pellerin, "Project Maven to Deploy Computer Algorithms to War Zone by Year's End," Department of Defense, July 21, 2017, https://www.defense.gov/News/News-Stories/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/.

60 percent accuracy rate: Katrina Manson, "AI Warfare Is Already Here," Bloomberg Businessweek, February 28, 2024, https://www.bloomberg.com/features/2024-ai-warfare-project-maven/?sref=gVdhVt7n.

84 percent of the time: Manson, "AI Warfare Is Already Here."

better than doctors: See, for example, Radboud University Medical Center, "AI Better Detects Prostate Cancer on MRI than Radiologists," ScienceDaily, June 12, 2024, https://www.sciencedaily.com/releases/2024/06/240612113341.htm#:~:text=Accurate%20Diagnosis&text=This%20first%20international%20study%20on,cancer%2C%20fifty%20percent%20less%20often.

In 2022, Project Maven: Nathan Strout, "Intelligence Agency Takes Over Project Maven, the Pentagon's Signature AI Scheme," C4ISRNET, April 27, 2024, https://www.c4isrnet.com/intel-geoint/2022/04/27/intelligence-agency-takes-over-project-maven-the-pentagons-signature-ai-scheme/.

Anduril: "Anduril's Lattice: A Trusted Dual Use—Commercial and Military—Platform for Public Safety, Security, and Defense," Anduril Industries, July 31, 2023, https://www.anduril.com/article/anduril-s-lattice-a-trusted-dual-use-commercial-and-military-platform-for-public-safety-security/.

Herman Kahn: Herman Kahn, On *Escalation: Metaphors and Scenarios* (Praeger, 1965).

revolution in intelligence affairs: Anthony Vinci, "The Coming Revolution in Intelligence Affairs: How Artificial Intelligence and Autonomous Systems Will Transform Espionage," *Foreign Affairs* (August 2020).

“collection on our competitors’”: Office of the President of the United States of America, “Fact Sheet: Biden–Harris Administration Outlines Coordinated Approach to Harness Power of AI for U.S. National Security,” October 24, 2024, https://www.whitehouse.gov/briefing-room/statements-releases/2024/10/24/fact-sheet-biden-harris-administration-outlines-coordinated-approach-to-harness-power-of-ai-for-u-s-national-security/.

Chapter 13: The Connectivity Competition

"Hi, Joel, it's Marty": Michelle Delgado, "From 'the Brick' to the iPhone, the Cellphone Celebrates 50 Years," *Smithsonian Magazine*, April 3, 2023, https://www.smithsonianmag.com/innovation/from-the-brick-to-the-iphone-the-cellphone-celebrates-50-years-180981910/.

This next-generation networking: World Economic Forum, "The Impact of 5G: Creating New Value Across Industries and Society," January 2020, http://www3.weforum.org/docs/WEF_The_Impact_of_5G_Report.pdf.

operates in 170 countries: Huawei Technologies, "Company Facts," Huawei, https://www.huawei.com/en/media-center/company-facts; *Forbes*, "Huawei," https://www.forbes.com/companies/huawei/?sh=68b062495d26.

stole intellectual property: "Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets," U.S. Department of Justice, February 13, 2020, https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-subsidiaries-charged-racketeering.

The U.S. government and others: "U.S. Officials Say Huawei Can Covertly Access Telecom Networks," *Wall Street Journal*, January 31, 2020, https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256; British Broadcasting Corporation, "Huawei: MPs Claim 'Clear Evidence of Collusion' with Chinese Communist Party," BBC News, https://www.bbc.com/news/technology-54455112.

Huawei has had a close relationship: Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," *Wall Street Journal*, December 25, 2019, https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

NSA reportedly infiltrated: David E. Sanger and Nicole Perlroth, "N.S.A. Breached Chinese Servers Seen as Security Threat," *New York Times*, March 23, 2014, https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html.

In the 2024 presidential election: Devlin Barrett, Jonathan Swan, and Maggie Haberman, "Chinese Hackers Are Said to Have Targeted Phones Used by Trump and Vance," October 25, 2024, https://www.nytimes.com/2024/10/25/us/politics/trump-vance-hack.html.

Chapter 14: Eyes Everywhere

notably named in a 2022 speech: William Burns, “The Role of Intelligence at a Transformational Moment,” Georgia Tech, April 14, 2022, https://www.cia.gov/static/Director-Burns-Speech-and-QA-Georgia-Tech.pdf.

900,000 CCTV cameras: Clarion Security Systems, “How Many CCTV Cameras Are in London,” 2022, https://clarionuk.com/resources/how-many-cctv-cameras-are-in-london/#:~:text=Research%20by%20Clarion%20Security%20Systems.

China may have a billion: Isabella Qian et al., “Four Takeaways from a Times Investigation into China’s Expanding Surveillance State,” *New York Times*, June 21, 2022, https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html.

researchers have shown: Zhou Man et al., “PrintListener: Uncovering the Vulnerability of Fingerprint Authentication via the Finger Fiction Sound,” arXiv, April 14, 2024, https://arxiv.org/abs/2404.09214.

ten centimeters: See, for example, Albedo, https://albedo.com; and EOI Space, https://eoi.space.

“the GEOINT Singularity”: Josef Koller, “The Future of Ubiquitous Realtime Intelligence: A GEOINT Singularity,” Aerospace Corporation, 2019.

guerrilla must move: Paraphrasing from Mao Zedong, *On Guerrilla Warfare* (1937).

private intelligence agency called the Pond: Mark Stout, “The Pond: Running Agents for State, War, and the CIA,” *Studies in Intelligence* 48, no. 3 (2004), https://web.archive.org/web/20070613113255/https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article07.html

after the Salt Typhoon hack: Raphael Satter and A. J. Vicens, “US Government Tells Officials, Politicians to Ditch Regular Calls and Texts,” Reuters, December 18, 2024, https://www.reuters.com/world/us/us-cyber-watchdog-tells-senior-officials-immediately-adopt-end-to-end-encryption-2024-12-18/.

Chapter 15: Cognitive Warfare

By the late 2010s: "Social Media and News Fact Sheet," Pew Research Center, September 17, 2024, https://www.pewresearch.org/journalism/fact-sheet/social-media-and-news-fact-sheet/.

In 2017, ByteDance: Matthew Miller, "China's Toutiao Is Buying Musical.ly in a Deal Worth $800M–$1B," TechCrunch, November 9, 2017, https://techcrunch.com/2017/11/09/chinas-toutiao-is-buying-musical-ly-in-a-deal-worth-800m-1b/?guccounter=1.

It then spent billions: Raheel Bakhsh, "TikTok's Secret to Viral Growth," Incentive Theory, Medium, June 12, 2020, https://incentivetheory.medium.com/tiktoks-secret-to-viral-growth-dcae8f6bcb9a.

by 2024, it had more than: TikTok Newsroom, "Celebrating Our Thriving Community of 150 Million Americans," TikTok, n.d., https://newsroom.tiktok.com/en-us/150-m-us-users; "How Many Users on TikTok? Statistics & Facts (2024)," SEO.ai (blog), https://seo.ai/blog/how-many-users-on-tiktok#; Andrew Ross Sorkin et al., "TikTok Sale to U.S. Companies Falls Apart," *New York Times*, March 12, 2024, https://www.nytimes.com/2024/03/12/business/dealbook/tiktok-house-ban.html.

TikTok collects a huge amount: "House Expected to Vote on Bill Banning TikTok," *New York Times*, March 13, 2024, https://www.nytimes.com/2024/03/13/us/politics/tiktok-ban-house-bill.html; Brian Fung, "TikTok Collects a Lot of Data. But That's Not the Main Reason Officials Say It's a Security Risk," CNN, March 24, 2023, https://www.cnn.com/2023/03/24/tech/tiktok-ban-national-security-hearing/index.html.

ByteDance has even been accused: Kate O'Flaherty, "All the Ways TikTok Tracks You and How to Stop It," *Wired*, October 23, 2021, https://www.wired.com/story/tiktok-data-privacy/.

it has been well reported that: See, for example, Kim Komando, "Protect Your Data: Why You Should Be Wary of TikTok," *USA Today*, June 29, 2023, https://www.usatoday.com/story/tech/columnist/komando/2023/06/29/tiktok-china-protect-your-data/70351963007/.

documents were leaked from ByteDance: Alex Hern, "Revealed: How TikTok Censors Videos that Do Not Please Beijing," *Guardian*, September 25, 2019, https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing.

"the basis of whether": "A Tik-Toking Timebomb: How TikTok's Global Platform Anomalies Align with the Chinese Communist Party's Geostrategic Objectives," Miller Center on Policing and Community Resilience and the Network Contagion Research Institute, December 2023, https://networkcontagion.us/wp-content/uploads/A-Tik-Tok-ing-Timebomb_12.21.23.pdf.

"The results revealed": "Information Manipulation on TikTok and Its Relation to American Users' Beliefs about China," Miller Center on Policing and Community Resilience and the Network Contagion Research Institute, January 2025, https://networkcontagion.us/wp-content/uploads/Peer-Reviewed-Paper-in-Press_Dec.-2024.pdf.

In another study by the same: "Information Manipulation on TikTok and Its Relation to American Users' Beliefs about China."

More than three-quarters of Gen Z: Ypulse, "Gen Z Is Officially Using TikTok More than Any Other Social Media Platform," June 5, 2023, https://www.ypulse.com/article/2023/06/05/gen-z-is-officially-using-tiktok-more-than-any-other-social-media-platform/.

nearly 40 percent of U.S. adults: Rebecca Leppert and Katerina Eva Matsa, "More Americans—Especially Young Adults—Are Regularly Getting News on TikTok," Pew Research Center, September 17, 2024, https://www.pewresearch.org/short-reads/2024/09/17/more-americans-regularly-get-news-on-tiktok-especially-young-adults/.

Freedom House: Sarah Cook, "The Chinese Communist Party's Latest Propaganda Target: Young Minds," Freedom House, April 2019, https://freedomhouse.org/article/chinese-communist-partys-latest-propaganda-target-young-minds.

Chinese vice-premier Ding Xuexiang: Zhao Yimeng, "China, Africa to Boost Education Development," *China Daily*, September 2024, https://www.chinadaily.com.cn/a/202409/09/WS66de34a2a3103711928a6bee.html.

Also, Chinese companies like Tencent: See, for example, Tage Kene-Okafor, "African Edtech Startup Ulesson Raises $15m, Backed by Nielsen Ventures and Tencent," Tech Crunch, December 2021, https://techcrunch.com/2021/12/09/african-edtech-startup-ulesson-raises-15m-backed-by-nielsen-ventures-and-tencent/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAFhqn8l5N0xjT1aK9fjrvwvZQgoRA-XrsywvHe02JVNBY__mtDqCqtCCJ7N81DENBkRbTSEAYN2SpSPJDkl8Gmovt3W3pCcmzkC-VZSbBsPLpQuDD8saDJaJ8Dxxiu6Pki1_5Isr-Ii3NruuQ9OOXsNYa7iF1erM4za0Hft4T1tX#:~:text=Sign%20In-,African%20edtech%20startup%20uLesson%20raises%20%2415M,by%20Nielsen%20Ventures%20and%20Tencent&text=As%20many%20edtech%20companies%20benefited,African%20startups%20were%20left%20out.

The tutoring site Tutor.com: Melissa Korn, "Chinese Company Now Owns Tutoring Firm Contracted by Military and Schools in US," *Wall Street Journal*, May 8, 2023, https://www.wsj.com/articles/princeton-review-and-tutor-com-are-now-owned-by-a-chinese-company-58ebea38.

DeepSeek does censor: Zeyi Yang, "Here's How DeepSeek Censorship Actually Works—And How to Get Around It," *Wired*, January 31, 2025, https://www.wired.com/story/deepseek-censorship/.

this firewall denies the Chinese: See, for example, United States Senate, Committee on Foreign Relations, *The New Big Brother—China and Digital Authoritarianism*, 116th Congress, 2nd Sess. (Washington, DC: GPO, 2020), https://www.foreign.senate.gov/download/2020-sfrc-minority-report_-the-new-big-brother—china-and-digital-authoritarianism.

U.S. tech giants Cisco and Juniper: "U.S. Internet Providers and the 'Great Firewall' of China," Council on Foreign Relations, https://www.cfr.org/backgrounder/us-internet-providers-and-great-firewall-china.

The United Front Work: Alexander Bowe, "China's Overseas United Front Work: Background and Implications for the United States," U.S.-China Economic and Security Review Commission, August 24, 2018, https://www.uscc.gov/sites/default/files/Research/China%27s%20Overseas%20United%20Front%20Work%20-%20Background%20and%20Implications%20for%20US_final_0.pdf.

When propaganda does: "Chinese Communist Party's US Repression Under Xi Jinping at APEC," *Washington Post*, 2024, https://www.washingtonpost.com/world/interactive/2024/chinese-communist-party-us-repression-xi-jinping-apec/.

in the original *Top Gun* film: PEN America, *Made in Hollywood, Censored by Beijing*, PEN America, 2015, https://pen.org/report/made-in-hollywood-censored-by-beijing/.

Cena's acknowledgment: Rob McMahon, "Actor John Cena Apologizes After Taiwan Comment," NBC News, July 23, 2021, https://www.nbcnews.com/news/world/actor-john-cena-apologizes-after-taiwan-comment-n1268526.

censor a high school: Stu Woo, "China Makes Sure Everyone Writes Taiwan's Name Just So—Even a Colorado High School," *Wall Street Journal*, September 10, 2021, https://www.wsj.com/articles/china-makes-sure-everyone-writes-taiwans-name-just-soeven-a-colorado-high-school-11631304386.

China has for years theorized: See, for example, Joseph Shullman, "The Future of China's Cognitive Warfare: Lessons from the War in Ukraine," Hudson Institute, June 14, 2022, https://www.hudson.org/national-security-defense/the-future-of-china-s-cognitive-warfare-lessons-from-the-war-in-ukraine#:~:text=What%20Is%20Cognitive%20Warfare%3F,legal%20means%20to%20achieve%20victory.%20Show%20drafts.

mind-control race: Annalee Newlitz, "A Brief, Weird History of Brain Washing," *MIT Technology Review* (April 2024), https://www.technologyreview.com/2024/04/12/1090726/brainwashing-mind-control-history-operation-midnight-climax/.

"intelligible word sequences": Jerry Tang et al., "Semantic Reconstruction of Continuous Language from Non-invasive Brain Recordings," *Nature Neuroscience* 26, no. 5 (2023), https://www.nature.com/articles/s41593-023-01304-9.

It's easy to see how: For more on this topic, see, for example, Nita Farahany, *The Battle for Your Brain* (St. Martin's Press, 2023).

"The Internet is the new battlefield": Quoted in Chun Han Wong, "A Xi Enforcer Is Revving Up China's Spy Machine—and Alarming the West," *Wall Street Journal*, November 9, 2024, https://www.wsj.com/world/china/a-xi-enforcer-is-revving-up-chinas-spy-machineand-alarming-the-west-6b87999f?mod=mhp.

Chapter 16: Hacking Minds

“My little scam”: Aldrich Ames, interview by Svetlana Savranskaya, “National Security Archive Cold War Interview,” Episode 21, George Washington University, https://nsarchive2.gwu.edu/coldwar/interviews/episode-21/aldrich5.html.

“it’s designed to sound natural”: Text generated by ChatGPT 4o, OpenAI, January 1, 2024.

“My voice is … **designed to convey”:** Text generated by ChatGPT 4o, OpenAI, January 1, 2024.

“I am a person who responds”: Text generated by ChatGPT 4o, OpenAI, January 2, 2024.

“Of course! Let’s explore”: Text generated by ChatGPT 4o, OpenAI, January 2, 2024.

a *New York Times* reporter: Kevin Roose, “A Conversation with Bing’s Chatbot Left Me Deeply Unsettled,” *New York Times*, February 16, 2023, https://www.nytimes.com/2023/02/16/technology/bing-chatbot-microsoft-chatgpt.html.

“**The supreme art of war”:** Sun Tzu, *The Art of War* (Capstone Publishing, 2010).

“its generative artificial intelligence”: Cade Metz, “OpenAI Says Russia and China Used Its A.I. in Covert Campaigns,” *New York Times*, May 30, 2024, https://www.nytimes.com/2024/05/30/technology/openai-influence-campaigns-report.html.

Chapter 17: Citizen Intelligence

At 12:31 p.m. on July 17: Dutch Safety Board, *Report MH17 Crash*, October 13, 2015, Netherlands Organisation for Applied Scientific Research TNO, Web Archive, https://web.archive.org/web/20151013141325/http://cdn.onderzoeksraad.nl/documents/report-mh17-crash-en.pdf.

Founded earlier that same year: For more on Bellingcat, see Eliot Higgins, *We Are Bellingcat: Global Crime, Online Sleuths, and the Bold Future of the News* (Bloomsbury Publishing, 2021).

By scouring social media posts: Bellingcat, "MH17—The Open Source Evidence," October 8, 2015, https://www.bellingcat.com/news/uk-and-europe/2015/10/08/mh17-the-open-source-evidence/.

Delphi, Indiana, in 2017: Aja Romano, "The Delphi Murders Were a Local Tragedy. Then They Became 'True Crime,'" Vox, March 6, 2023, https://www.vox.com/culture/23619617/delphi-murders-updates-reddit-true-crime.

playing a part in tracking: Johnny Nhan, Laura Huey, and Ryan Broll, "Digilantism: An Analysis of Crowdsourcing and the Boston Marathon Bombings," *British Journal of Criminology* 57, no. 2 (March 1, 2017): 341–61, doi.org/10.1093/bjc/azv118.

There is even a group: Howard Altman, "'People's Satellite' Helped Ukraine Hit over 1,000 Targets Spy Agency Says," *War Zone*, June 26, 2024, https://www.twz.com/news-features/peoples-satellite-helped-ukraine-hit-over-1000-targets-spy-agency-says.

In 2009, the Defense Advanced: DARPA, "Red Balloon Challenge," Achttps://www.darpa.mil/about-us/timeline/network-challenge.

"to dramatically enhance": Office of the Director of National Intelligence, "Intelligence Advanced Research Projects Activity, Aggregative Contingent Estimation," IARPA, n.d., https://www.iarpa.gov/index.php/research-programs/ace.

Tetlock's team used: Philip E. Tetlock and Dan Gardner, *Superforecasting: The Art and Science of Prediction* (Crown Publishers, 2015).

a range of foreign actors: Office of the Director of National Intelligence, "30 Days Until Election 2024," Foreign Malign Influence Center, October 2024, https://www.dni.gov/files/FMIC/documents/ODNI-Election-Security-Update-20241007.pdf.

Nextdoor is a hyperlocal: Nextdoor, a neighborhood social network, About page, https://about.nextdoor.com/.

Waze: Google Help, "Who Is Waze Designed For?" https://support.google.com/waze/answer/6071177?hl=en#zippy=%2Cwho-is-waze-designed-for.

PulsePoint: "PulsePoint Respond: Overview," PulsePoint Foundation, https://www.pulsepoint.org/pulsepoint-respond#overview.

Citizen: Citizen, https://citizen.com/about.

PolitiFact: See, for example, https://www.politifact.com and https://www.snopes.com. RAND has put together a comprehensive list of such sites here: https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html.

Center for an Informed Public: Steven Lee Myers and Stuart A. Thompson, "Disinformation Watchdogs Are Under Pressure. This Group Refuses to Stop," *New York Times*, November 1, 2024,

https://www.nytimes.com/2024/11/01/technology/election-disinformation.html.

have been considered partisan: Myers and Thompson, “Disinformation Watchdogs Are Under Pressure. This Group Refuses to Stop.”

politically charged: See, for example, Steven Lee Myers and Sheera Frenkel, “GOP Targets Researchers Who Study Disinformation Ahead of 2024 Election,” *New York Times*, June 19, 2024, https://www.nytimes.com/2023/06/19/technology/gop-disinformation-researchers-2024-election.html.

In the lead-up to: Joshua C. Huminski, “Russia, Ukraine, and the Future Use of Strategic Intelligence,” *PRISM* 10, no. 3 (September 7, 2023), National Defense University Press, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3511951/.

Chapter 18: Philosopher Spy

The Martians sent for samples: M. W. Rowe, *J. L. Austin: Philosopher and D-Day Intelligence Officer* (Oxford University Press, 2023).

The Martians were led: Rowe, *J. L. Austin*; Thomas Nagel, "Leader of the Martians," *London Review of Books* 45, no. 17 (September 7, 2023), http://lrb.co.uk/the-paper/v45/n17/thomas-nagel/leader-of-the-martians?utm_source=pocket_shared.

"Joshua son of Nun": Joshua 2:1, Bible, New International Version.

"Whatever the Party holds": George Orwell, *1984* (Signet Classic, 1961).

"most voters tend to": "AI Will Change American Elections, but Not in the Obvious Way," *Economist*, August 31, 2023, https://www.economist.com/united-states/2023/08/31/ai-will-change-american-elections-but-not-in-the-obvious-way.

"truth's cash value": William James, *On Pragmatism: A New Name for Some Old Ways of Thinking* (Longmans, Green, and Co., 1907).

Rorty: Richard Rorty, *Pragmatism as Anti-Authoritarianism* (Belknap Press, 2021).

Chapter 19: Intelligence 4.0

“I only regret”: There is no single official source for this quote as recorded in common lore.

OceanofPDF.com

Acknowledgments

In movies, we're captivated by the vision of the lone intelligence officer. But in reality, as he walks down a dark alleyway, that intelligence officer is backed up by many other people. The same goes for authors. The single name on a book's cover has been aided by many others. I am eternally grateful to all those who helped me put this book into your hands.

Thank you to Tim Duggan, Zoë Affron, and the team at Henry Holt for believing in this book and for their invaluable editorial comments and support. I also extend my gratitude to the Smith Richardson Foundation and the foundation's president, Marin Strmecki, for their generous grant, which enabled me to research and write the initial version of this book. My thanks as well to the Center for a New American Security, with particular appreciation to Paul Scharre, Jake Penders, and others who supported the SRF grant and my own work over the years.

A special thank-you to my agent, Toby Mundy, whose guidance has been instrumental. From helping to shape the initial concept and title to refining the content and cover, your fingerprints are all over this, and it's been a privilege to work with you.

I'm especially thankful to Shannon O'Neil, who was central to the writing process and who provided immensely valuable inputs and edits that elevated each draft and made every page stronger. It was a true pleasure to work with her.

Thank you to Nadia Schadlow, who first encouraged me to write this book. She was enormously helpful in thinking it through and providing insightful edits and ideas throughout the process.

I truly couldn’t have written this without the help of Robert Cardillo, who took a leap of faith on me at the NGA and who has been incredibly helpful in honing my thinking around intelligence both broadly and specifically for this book.

Thank you to others who helped me in conversations, thinking, research, with edits, and otherwise in making this idea a reality, including Josh Alcorn, Jason Bruzdzinski, Sue Gordon, Steve Hunnewell, Kennon Kincaid, Matt McKnight, H. R. McMaster, Ed Mornston, James Mulvenon, Jake Newman, Lyndon Oh, Tony Porter, Jason Providakes, Matt Ruane, Daniel Rudder, Will Schlickenmaier, Dick Szafranski, Hamlet Yousef, and Justin Zeefe. Also, special thanks to Marin Halper who challenged me with excellent critiques and ideas.

Thank you to Courtney for being my biggest supporter. Coming from outside this world, she acted as the reader I hoped to speak to and brought many insights I had been too close to the subject matter to see myself. More than that, her understanding, encouragement, and care kept me going.

To my father, who provided an example of service that led me here and was a key support during the writing of this book.

And most important, to my son, who inspired me to reconsider and reimagine what was important, from being “OP” to Nathan Hale to understanding who we are here to protect. My deepest gratitude goes to him and his generation, to whom we will one day pass the baton to secure our nation and our democracy.

OceanofPDF.com

Index

The index that appeared in the print version of this title does not match the pages in your e-book. Please use the search function on your e-reading device to search for terms of interest. For your reference, the terms that appear in the print index are listed below.

The index that appeared in the print version of this title does not match the pages in your e-book. Please use the search function on your e-reading device to search for terms of interest. For your reference, the terms that appear in the print index are listed below.

A-12 Oxcart
Abbottabad, Pakistan
A/B testing
Advanced Intelligence Section (“Martians”)
Aerospace Corporation
Afghanistan
  Soviet war in
  U.S. war in
Africa
African National Congress
Aggregative Contingent Estimation (ACE)
Agrarian Reform Law (Guatemala, 1952)
Agriculture Department (USDA)
AI, Automation, and Augmentation (AAA)
AI agent model
AI Assurance and Discovery Lab
Aim 9X Sidewinder missile
Aimpoint
Air Combat Evolution (ACE)
AK-47 assault rifles
Alexa
Algorithmic Warfare Cross-Functional Team
algorithms
Alibaba
Alphabet
Al-Qaeda
Amazon
Amazon Web Services
American students in China
Ames, Aldrich
Amnesty International
analysis

Anaximander
Andreessen Horowitz
Andrews Air Force Base
Anduril
Angleton, James Jesus
Ansar Allah. *See* Houthis
Anthem
Anthropic
anti-access/area denial (A2AD)
Arab Spring
Àrbenz, Jacobo
Arctic ice melts
Area 51
Arendt, Hannah
Aristotle
Artemis
artificial general intelligence (AGI)
artificial intelligence (AI). *See also specific applications and types*
Art of War, The (Sun Tzu)
Assad, Bashar al-
Assange, Julian
assassinations
asymmetric adversaries
AT&T
atomic bomb
Austin, J. L.
Australia
authoritarians (totalitarians)
automation
autonomous systems
Axis powers

B-52 bomber
Baghdad
Bank, Aaron
Ban Ki-moon
barbell approach
battlefield brain
Baudrillard, Jean
BBC
Beijing
Beijing Kunlun
Bellingcat
Bell Labs
Belt and Road Initiative
Bentham, Jeremy
Berlin
Berlin Wall, fall of
BGI Genomics
Bible
Biden, Joseph
bin Laden, Osama
Biological Command (BIOCOM)
biotech
biothreats
Bissell, Richard, Jr.
black budget
Black Chamber
BlackSky

Blackwater
Blank, Steve
Bloomberg Terminal
Blue Origin
Boeing
Bond, James (fictional character)
Boston Marathon bombers
brain-computer interface (BCI)
Bridgewater Associates
Britain
British Department of Health and Social Care
British Secret Intelligence Service (SIS). *See also* MI6
Buk surface-to-air missile
Burma (Myanmar)
Burns, William
Burton, Richard Francis
Bush, George H. W.
Bush, George W.
ByteDance

C-119J Flying Boxcar
Caesar, Julius
Canada
Capella Space
Cardillo, Robert
Carell, Steve
Carmichael, William
Carthage
cell phones (smartphones)
Cena, John
censorship
Center for an Informed Public
Center on Climate Change and National Security
Centers for Disease Control and Prevention (CDC)
Central Asia
Central Intelligence Agency (CIA). *See also specific units*
Chang, Jacky
Chang'e 4
ChatGPT
Chemical and Biological Warfare Programme (South Africa)
Chen Yixin
Child, Julia
China
China Aerospace Science and Industry Corporation
China Association for International Friendly Contact
China Commercial Space Alliance
China Development Bank
China Harbour Engineering Company
China Mobile
China National GeneBank
Chinese Communist Party (CCP)
Chinese Intelligence Bureau of the Joint Staff Department
Chinese Ministry of State Security (MSS)
Chinese navy
Chinese People's Liberation Army (PLA)
Chinese state-owned enterprises
Chinese Students and Scholars Association
Chinese students in the United States
Church Committee

Churchill, Winston
Cisco
citizen intelligence
Citizen (mapping platform)
Clapper, James
classification
climate crisis
Clinton, Bill
Clinton, Hillary
closed-circuit television (CCTV)
Coast Guard intelligence
cognitive warfare
Cold War
Cole, USS
Colossal Laboratories and Biosciences
Columbia University
Columbus, Christopher
Commerce Department
commercial companies
commercial data
Committee of Secret Correspondence
Communications Division (OSS)
communications intelligence (COMINT)
Community Notes
compartmentalization
Complete Genomics
computer vision
confidential classification
Confucius Institute
consumer data
Continental Army
Continental Congress
Contingency Fund for Foreign Intercourse
Controlled Access Programs (CAP)
Controlled Unclassified Information
Conversation, The (film)
Cooper, Martin
Cooperative Research and Development Agreements
Coppola, Francis Ford
CORONA program
counterintelligence (CI)
counterterrorism
covert action
covert influence campaigns
Covid-19
Covid-19 tests
Creech Air Force Base
Crimea
CrimeCon
CRISPR-Cas 9
crowdsourcing
Cruise, Tom
cryptocurrency thefts
Cuba
CubeSat
Cukor, Drew
Cultural Revolution
cyberattacks
Cyber Command (CYBERCOM)

cybersecurity

Dalio, Ray
DALL-E
Darfur
dark web
DARPA Network Challenge
data analysis
Data and Digital Innovation Directorate (NGA)
databases
data collection
Data Corps (NGA)
data encryption
Dayton, Elias
D-Day
DeepSeek
Defense Advanced Research Projects Agency (DARPA)
Defense Department (DoD; Pentagon)
Defense Intelligence Agency (DIA)
de Gaulle, Charles
Delphi, Indiana, murders
democracies
democratization of intelligence
Democrats
Deng Xiaoping
denial-and-deception campaigns
Descartes, René
Die Another Day (film)
DigitalGlobe
Ding Xuexiang
director of central intelligence (DCI)
director of national intelligence (DNI)
Discoverer 14. *See also* CORONA program
disease monitoring
disinformation. *See also* covert influence campaigns
distributed denial-of-service (DDoS) attacks
DJI drone feeds
DNA samples
Do Anything Now (DAN)
Domestic Security Alliance Council
Donetsk People's Republic
Donovan, William
Douyin
Down syndrome
drones
Drug Enforcement Agency
Dulles, Allen
Dulles, John Foster
Dynetics

Eastman Kodak
economic intelligence
Economist
Edwards syndrome
Egypt, Ancient
Eisenhower, Dwight D.
Election Integrity Network
elections
  of 2016

of 2020
of 2024
electronic intelligence (ELINT)
electro-optical/infrared (EO/IR) imagery
Elroy Air Chaparral C1
Emirati Intelligence
Enemy of the State (film)
Energy Department
Engel, Joel
Enigma
Entity List
Equifax
Ericsson
Ethiopia
Europe
European Parliament
European Union

F9 (film)
F-16 jet
F-22 Raptor jet
F-35 Lightning jet
Facebook
Falcon 9 rocket
Falcon Heavy rocket
Falun Gong
Fanhui Shi Weixing
Farm, the
Federal Acquisition Regulations (FAR)
Federal Aviation Administration (FAA)
Federal Bureau of Investigation (FBI)
Federal Reserve
Federal Security Service (FSB, Russia)
film bulk acoustic resonator (FBAR)
financial data
First Amendment
Five Eyes
5G networks
Flat Earthers
Food and Drug Administration (FDA)
Foreign Malign Influence Center
Foreign Policy
Fort Detrick
France
Franco, James
Freedom House
Free French Forces
Freemasons
French Resistance
Friendster
Fulda Gap

Generation Alpha
Generation X
Generation Z
generative AI
genetic data
genetic engineering
genetic intelligence

genetic sequencing
Genomics England
GEOINT Singularity
geospatial intelligence (GEOINT)
Germany
  Nazi
  post–World War II
Gibson, William
Ginkgo Bioworks
Global Disease Detection Operations Center
Global War on Terror
Goethe Institute
Good Judgment Project
Google
Google+
Google Earth
Google Maps
Gorbachev, Mikhail
GPS
Great Firewall
Great Game
Greeks, Ancient
Grindr
Grombach, Jean Valentin
GRU
Guatemala
Gutenberg

Hackman, Gene
Hale, Nathan
Hamas
Hambantota Port, Sri Lanka
Harris, Kamala
Harvard University
Hawaii
HawkEye 360
Hearst, William Randolph
He Jiankui
Hellfire missiles
Her (film)
Hezbollah
Higgins, Eliot
High Mobility Artillery Rocket System (HIMARS)
HIV
HK416 rifle
Homeland Security Department
Hong Kong
Hoover, J. Edgar
Houthis (Ansar Allah)
Huawei Technologies
Human Genome Project
human intelligence (HUMINT)
Human Rights Watch
Hunan Province
Hussein, Saddam
Hwasong-18 ICBM
hydrogen bomb
hypersonic missiles
hyperspectral sensors

ICEYE
IEDs
ImageNet
Inception (film)
India
Information Sharing and Analysis Centers (ISACS)
In-Q-Tel
Instagram
Intelligence Advanced Research Projects Activity (IARPA)
Intelligence and Research, Bureau of (INR)
Intelligence and Security Command (INSCOM)
intercontinental ballistic missiles (ICBMs)
Internal Revenue Service (IRS)
International Crisis Group
International Lunar Research Station
International Monetary Fund
International Olympics Committee
International Space Station
internet
Internet of Things (IoT)
Internet Research Agency (IRA)–63
Interview, The (film)
INTs
IP thefts
Iran
Iraq
  U.S. war vs.
Iron Curtain
Iron Man (comics and movies)
ISIS
Islamic Revolutionary Guard Corps (IRGC)
Israel
  Hamas war vs.
Italy, Fascist

James, William
Japan
  World War II and
J.A.R.V.I.S.
JASON advisory group
Jedburghs
Jigsaw
Johnson, Clarence “Kelly”
Joint All-Domain Command and Control (JADC2)
Joint Chiefs of Staff
Joint Intelligence Objectives Agency
Juniper Networks
Justice Department

K-129 submarine
Kandahar, Afghanistan
Kelly, Kevin
Keyhole
KGB
Khallad (Walid bin Attash)
Khan Academy
Kickstarter
Kim Jong-un
Kissinger, Henry

Knowlton’s Rangers
Kurds

Lambertsen, Christian
Lambertsen Amphibious Respiratory Unit (LARU)
Landres-et-Saint Georges, Battle of
Langer, William
large language models (LLMs)
Lattice battlefield brain technology
League of Nations
Lebanon
Leibniz, Gottfried W.
Level 7 up-armored, lo-pro vehicles
LGBTQ
Li, Fei-Fei
Libyan civil war
LIDAR (light detection and ranging)
LinkedIn
Litvinenko, Alexander
Lockheed Martin
London
LSD
Lundhal, Arthur
Luttwak, Edward

Ma, Jack
MacArthur, Douglas
machine learning
machine learning poisoning
Made in China 2025
Maine, USS (ship)
Malaysia
Malaysian Airlines Flight MH17
malware
Mao Zedong
Maritime Unit
Marriott hotels
Mars
Marshall Plan
Matrix, *The* (film)
Maxar
McCarthy, Joseph
McLuhan, Marshall
measurements and signature intelligence (MASINT)
Measurements of Earth Data for Environmental Analysis (MEDEA)
Meta
MI5
MI6
MI14
Microsoft
Microsoft Bing chatbot
Midjourney
MiG fighter jets
Mihdhar, Khalid al-
military intelligence
Millennials
Milley, Mark
Mission Impossible (film)
MITRE

MIT Red Balloon Challenge Team
MK-ULTRA
mobile movement data
Mobile TeleSystems
Moon
Moscow Rules
Mossad
Motorola
MQ-1 Predator
MQ-9 Reaper
MQ-25 Stingray
MRI images
Musical.ly
Mussolini, Benito
MySpace

Nangarhar Province, Afghanistan
National Aeronautics and Space Administration (NASA)
National Center for Medical Intelligence
National Commission on Terrorist Attacks Upon the United Sates (9/11 Commission)
National Counterintelligence and Security Center (NCSC)
National Counterterrorism Center (NCTC)
National Economic Defense Center (NEDC, proposed)
National Geospatial-Intelligence Agency (NGA). *See also specific units*
National Imagery and Mapping Agency (NIMA; *later* NGA)
National Intelligence Law (China, 2017)
National Photographic Interpretation Center
National Reconnaissance Office (NRO)
National Science Foundation (NSF)
national security, expanding concept of
National Security Act (1947)
National Security Agency (NSA)
National Security Council (NSC)
National Security Memorandum on Artificial Intelligence (2024)
National Security Strategy (Trump)
National Space Intelligence Center (Space Delta 18)
National Strategy for Information Sharing and Safeguarding (Obama)
NATO
natural disasters
Nature Neuroscience
Netflix
Network Contagion Research Institute
network intelligence
Neuralink
Newsmax
New York State
New York Times
New Zealand
Nextdoor
Nietzsche, Friedrich
Nile River
9/11 attacks
9/11 Commission Report
1984 (Orwell)
Nixon, Richard
Nokia
Nolan, Christopher
Non-classified Internet Protocol Network (NIPRNet)
Northern Alliance

North Korea
Northwest Passage
Novana
nuclear weapons

Obama, Barack
Office of Analysis (NGA)
Office of Censorship
Office of Commercial and Economic Analysis (OCEA)
Office of Naval Intelligence
Office of Personnel Management (OPM)
Office of Strategic Services (OSS)
Office of the Coordinator of Information (COI)
Office of the Director of National Intelligence (ODNI)
Office of Ventures and Innovation
OpenAI
Open Source Enterprise
open-source intelligence, (OSINT)
operational security (OPSEC)
Operation Paperclip
Opportunity Zones
Optimus robot
Oracle
Orwell, George
Other Transaction Authorities (OTAs)
Oxford University

Pakistan
Palantir
pandemics
panopticon
Papperger, Armin
Patau syndrome
Pathfinder program
Pearl Harbor attacks
Perplexity
Persian Empire
Personal Identifying Information (PII)
Personal Information Protection Law (China, 2021)
Pew Research Center
phishing attacks
Phoenicians
Phoenix, Joaquin
Planet company
PolitiFact
polygraph
Pond, the
Powell, Colin
Powers, Francis Gary
President’s Daily Brief (PDB)
Prigozhin, Yevgeny
Princess Bride, The (film)
Princeton Review
Project Azorian
Project BLACKFLAG
Project Coast
Project IMPACT
Project Maven
Project Socrates

propaganda. *See also* covert influence campaigns; disinformation
proxy insurgencies
public-private partnerships
PulsePoint
Putin, Vladimir
Putnam, Hilary
Python

Quds Force
Quran

Rajapaksa, Mahinda
Rambo (film)
RAND
ransomware
rare earth minerals
Reagan, Ronald
Realism theory
Reddit
Redstone missile
Reiner, Rob
Ren Zhengfei
Reporters Without Borders
Republicans
Research and Analysis branch (R&A; OSS)
Research and Development branch (R&D; OSS)
Revere, Paul
Revolutionary War
Rheinmetall
Ridley, Matt
Ries, Eric
RocketLab
rockets
Rogen, Seth
Rome, Ancient
Roosevelt, Franklin D.
Roper, Will
Rorty, Richard
Russia
  Ukraine war and. *See also* Soviet Union
Russian Empire, pre-1917
Rutgers University Miller Center on Policing and Community Resilience
Rwanda

Sadr City
Salt Typhoon
SAP/CAP compartment
satellite imagery 112
satellites
Saturn V rocket
Saudi Arabia
science and technology
science and technology intelligence (S&TI)
SCIFs (sensitive compartmented information facilities)
Secret classification
Secret Intelligence division (SI; OSS)
Securities and Exchange Commission (SEC)
Securities Regulatory Commission (China)
Sedition Act (1918)
semiconductors

Senior Steering Group
sensitive compartmented information (SCI)
sensors
Shanahan, Jack
Signal
signals intelligence (SIGINT)
SIG Sauer 226 sidearm
Silicon Valley
Simkhai, Joel
Simulacra and Simulation (Baudrillard)
singularity war
Sixty-ninth New York Infantry Regiment
Skripal, Sergei
Skyworks Solutions
Small Business Innovation Research (SBIR)
smartwatches
Smith, Will
Snapchat
Snopes
Snowden, Edward
social credit system
social media
social networks
Social Security numbers
Socrates
Soleimani, Qasem
Sony Pictures Entertainment
Sora
South Africa
South China Morning Post
South China Sea
Southern University of Science and Technology (Shenzhen)
Soviet Communist Party, Central Committee
Soviet Union (USSR). *See also* Russia
  Afghanistan invaded by
  fall of
Space Age
space-based intelligence. *See also* satellites
Space Delta 7
Space Delta 18
space domain awareness (SDA)
Space Force
Space Race
SpaceX
Spain
Spanish-American War
Spanish Civil War
Special Access Programs (SAP)
Special Operations division (SO; OSS)
Special Operations Executive (SOE), British
Sputnik 1
Sri Lanka
Stalin, Joseph
Stanford University
Starlink satellite
Starshield unit (SpaceX)
Starship rocket
Stasi
State Department

Stimson, Henry L.
Stinger surface-to-air missiles
strategic competition doctrine
strategic intelligence
Strategic Services Unit (SSU)
strategy, paradox of
Sudan
Sun Tzu
superintelligence
supply chains
surveillance
Svalbard Island
SVR
swarms
Switzerland
synthetic aperture radar (SAR)
synthetic biology
Syria

T-80 tank
tactics, techniques, and procedures (TTPs)
Taiwan
Taliban
targeting officer
Tearline
telecommunications. *See also* cellphones; internet
telecom networks
Tencent
Tenet, George
Terminator films
terrorism
Tesla
Tetlock, Philip
texting
Thailand
Tiananmen Square Massacre
Tianjin University
Tibet
Tigray war
TikTok
T-Mobile
Tocqueville, Alexis de
Top Gun (film)
Top Gun: Maverick (film)
Top Secret classification
Top Secret/SCI clearance
Transportation Department
transporter erector launchers (TELs)
Treasury Department
triangulation
Trojan horses
Trotsky, Leon
Truman, Harry
Trump, Donald J.
Truth and Reconciliation Commission (South Africa)
Tumblr
Turner, Stansfield
Tutor.com
TVBS news station

23andMe
Twitter (*later* X)

U-2 plane
Ubico, Jorge
ubiquitous technical surveillance (UTS)
Uighurs
Ukraine
  Russian war vs.
ULTRA program
Umbra
United Front Work Department (China)
United Fruit Company
United Nations
  Security Council
University of Pennsylvania
University of Southern California
University of Texas
University of Washington
U.S. Air Force
U.S. Air Force intelligence
U.S. Army
U.S. Army Military Intelligence Division
U.S. Army Special Forces (Green Berets)
U.S. Congress
U.S. Geospatial Intelligence Foundation (USGIF)
U.S. House of Representatives
  Intelligence Committee
U.S. Marine Corps
U.S. military service members
U.S. Navy
U.S. Navy SEALs
U.S. Senate
  Intelligence Committee

V-1 buzz bomb
V-2 rocket
Vance, JD
Vandenberg Air Force Base
Verizon
Victoria, queen of England
Vietnam
Vikings
Von Braun, Wernher
Von Kármán crater (Moon)

Waffen SS
Wagner Group
Wall Street Journal
War Department
Washington, George
Washington Post
whole-of-government approach
whole-of-nation approach
whole-of-planet approach
whole-of-society approach
WikiLeaks
Wikipedia
Wired
Wolff, Karl

Work, Bob
World Anti-Doping Agency
World Bank
World Factbook
World Health Organization
World War I
World War II
World War III
Wuhan Central Hospital

X (*formerly* Twitter)
X-2 office
X-62A fighter jet
Xi Jinping
Xinjiang Province

Yemen
YouTube
Yutu-2 probe

Zelenskyy, Volodymyr
Zenit satellite program
Zhang Hao
ZTE Corporation

OceanofPDF.com

About the Author

Dr. Anthony Vinci served as the first Chief Technology Officer at the National Geospatial-Intelligence Agency (NGA). Earlier in his career he served in Iraq, Africa, and Asia. After leaving the world of intelligence, Vinci became an executive at a private equity firm and CEO of an AI company. He is an Adjunct Senior Fellow at the Center for a New American Security (CNAS) and received his PhD in International Relations from the London School of Economics. You can sign up for email updates here.

OceanofPDF.com

Thank you for buying this
Henry Holt and Company ebook.

To receive special offers, bonus content,
and info on new releases and other great reads,
sign up for our newsletters.

Sign Up

Or visit us online at
us.macmillan.com/newslettersignup

For email updates on the author, click here.

OceanofPDF.com

The Fourth Intelligence Revolution: The Future of Espionage and the Battle to Save America.
Copyright © 2025 by Anthony Vinci. All rights reserved. For information, address Henry Holt and Co., 120 Broadway, New York, N.Y. 10271.

www.henryholt.com

Cover design by Emily Mahar
Cover image © Skorzewiak / Shutterstock

Library of Congress CIP data for the print edition is available.

e-ISBN 9781250370891

The publisher of this book does not authorize the use or reproduction of any part of this book in any manner for the purpose of training artificial intelligence technologies or systems. The publisher of this book expressly reserves this book from the Text and Data Mining exception in accordance with Article 4(3) of the European Union Digital Single Market Directive 2019/790.

First Edition 2025

Our ebooks may be purchased in bulk for promotional, business, educational, and specialty retail/wholesale use. Please contact MacmillanSpecialMarkets@macmillan.com.

The opinions and views expressed in this book are the author's own and do not authenticate content or reflect the opinions or views of the intelligence community or United States government nor any companies or other organizations the author may have been involved with.

OceanofPDF.com

Contents

Title Page
Copyright Notice
Dedication
Prologue
Introduction

1. The Heroic Age
2. The Golden Age
3. The Chaotic Age
4. Asymmetric Adversaries
5. Enemy Number One
6. Embracing Economic Espionage
7. From National Security to Global Security
8. The Final Frontier of Intelligence
9. Genetic Espionage
10. The Rise of AI
11. From Augmenting to Automating Intelligence
12. Singularity War
13. The Connectivity Competition
14. Eyes Everywhere
15. Cognitive Warfare
16. Hacking Minds
17. Citizen Intelligence
18. Philosopher Spy
19. Intelligence 4.0

Notes
Acknowledgments
Index
About the Author
Copyright

OceanofPDF.com